Microsoft Windows Netzwerke

SCHULNETZ

Laborübungen

IMPRESSUM

Die im Laborbuch „Microsoft Windows -Netzwerke“ beschriebenen Laborübungen wurden im Rahmen der Fortbildungsinitiative SCHULNETZ zur Qualifizierung von Systembetreuerinnen und Systembetreuern von IT-Multiplikatoren erarbeitet.

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Dokumentation:	Peter Botzenhart, Akademie Dillingen
URL:	http://alp.dillingen.de/schulnetz
Mail:	p.botzenhart@alp.dillingen.de
Stand:	Oktober 2022

Inhaltsverzeichnis

Laborübung 01 - INSTALLATION DES HYPER-V HOSTS

Szenario

Der Windows Host mit der Hyper-V Rolle soll als Grundlage für die Lehrgangsstruktur installiert werden.

kurz & knapp

- Installation des Hosts
- Systemaktualisierung
- Grundkonfiguration

Vorbereitung

- Aktuelles Windows Server ISO-Image

Aufgaben

1. Überprüfen Sie im BIOS/UEFI, ob die Unterstützung für die Virtualisierungstechnologie aktiviert ist.
2. Installieren Sie Windows Server 2022 **mit Hyper-V Rolle:**
   Windows Server 2022 wird mit der Rolle Hyper-V auf einem physikalischen PC (Host System) installiert.
3. Überprüfen Sie, ob **Updates** für das Host System zur Verfügung stehen und installieren Sie diese.
4. Überprüfen Sie im **Gerätemanager** die korrekte Installation aller Hardwarekomponenten und installieren Sie bei Bedarf Gerätetreiber nach.
5. Konfigurieren Sie die **Netzwerkeinstellungen** an Ihrem Computer entsprechend den Erfordernissen (statische IP-Adresse, korrektes Gateway, DNS-Server).
6. Überprüfen Sie die Netzwerkfunktionalität mit:
   - *ipconfig /all*
   - *ping* auf das Gateway und den DNS-Server
   - *ping* auf www.alp.dillingen.de (Überprüfung der Namensauflösung)
7. Überprüfen Sie in der Ereignisanzeige, ob Warnmeldungen oder **Fehler** vorliegen und versuchen Sie, die Fehler zu beheben.

Hinweise

Virtualisierungseinstellungen im BIOS/UEFI

Einstellungen finden sich bei den Eigenschaften der CPU und in den Sicherheitseinstellungen

Verwaltungswerkzeuge unter Windows

Schnellzugriff (Win + X)

Troubleshooting im Netzwerk

`ipconfig /all`	Anzeige der IP-Konfiguration des Rechners.
`ping alp.dillingen.de`	Überprüft eine Verbindung auf IP-Ebene.
`arp -a/-d`	(Address Resolution Protocol) Liest/Löscht die Tabelle mit den Zuordnungen von IP-Adressen zu MAC-Adressen im lokalen Netz.
`netstat -n/-c`	Bestehende Netzwerkverbindungen werden angezeigt bzw. Cache wird gelöscht.

Virtualisierung

Bei der Virtualisierung werden mit Hilfe eines Hypervisors die tatsächlichen Ressourcen auf verschiedene virtuelle Maschinen (VM) aufgeteilt. Technischer gesprochen erzeugt ein Hypervisor eine Abstraktionsschicht zwischen der tatsächlich vorhandenen Hardware und weiteren zu installierenden Betriebssystemen. Solche Systeme erlauben es, eine virtuelle Umgebung (Hardwareressourcen, wie z. B. CPU, Arbeitsspeicher, Festplattenplatz…) als virtuelle Maschinen zu definieren.

Zur Unterscheidung von echter und virtueller Umgebung wird die echte Umgebung als **Host** (Gastgeber oder Wirt) und die virtuelle Umgebung als Gast bezeichnet.

Laborübung 02 - VORBEREITEN DER LABORUMGEBUNG

kurz & knapp

- Hyper-V Rolle
- Windows Serverumgebung
- Virtual Box

Szenario

Auf dem Windows Host soll die Hyper-V Rolle als Grundlage für die Lehrgangsstruktur konfiguriert werden. Anschließend wird Windows Server in einer VM installiert und virtuelle Windows Clients mit Hilfe von Virtual Box auf dem Desktop System als Host erstellt.

Vorbereitung

- Aktuelles Windows Server ISO-Image
- Aktuelles Windows 10/11 ISO-Image

Hinweise

Virtuelle Maschinen

Virtuelle PCs (VMs) bestehen üblicherweise aus einer Festplattendatei und einer Konfigurationsdatei. Diese können manuell oder per Softwaredialog auf dem jeweiligen Host hinzugefügt werden. Die zu importierenden VMs sollten keine Schnappschüsse enthalten.

USB - Geräte

Sowohl an Virtual Box als auch an Hyper-V können am Host verbundene USB-Geräte durchgereicht werden.

Virtual Box

Eine Anleitung zu Virtual Box ist auf den Schulnetzseiten erhältlich:

https://schulnetz.alp.dillingen.de/materialien/Virtualbox.pdf

Die Windows Clients sollen die Netzwerkeinstellungen „Netzwerkbrücke“ haben.

Laborübung 03 - REMOTEADMINISTRATION DES SERVERS

kurz & knapp

- Erstkonfiguration
- Firewall Einstellungen
- Remotedesktop

Szenario

Zur Administration des Servers sollen möglichst komfortable Zugänge und Werkzeuge bereitgestellt werden. Die Erstkonfiguration des Servers soll abgeschlossen sein, und eine Remoteverwaltung über das lokale Netzwerk möglich sein.

Aufgaben

1. Erstkonfiguration des Servers im Servermanager:
   - Netzwerkeinstellungen (statische IP-Adresse, Firewall)
   - Sinnvoller Computername (max. 15 Zeichen)
   - Remote Verwaltung
   - Windows-Updates (evtl. für Kursdauer aussetzen)

Remote-Administration

2. Ermöglichen Sie am Server die Remotedesktopverbindung und verbinden Sie sich von Ihrem Administrationsrechner (als Administrator) aus mit dem Server.

Systemsicherung

3. Erstellen Sie ein erstes Backup Ihrer Grundinstallation.

Hinweise

Netzwerkstandorte

Der Netzwerkstandort bestimmt die Firewall-Regeln. Die Remotedesktopverbindung ist standardmäßig nur innerhalb eines privaten Netzwerks möglich.

Netzwerkstandort ändern mit der Powershell

```
PS C:\> Get-NetConnectionProfile


Name             : Netzwerk
InterfaceAlias   : Ethernet
InterfaceIndex   : 4
NetworkCategory  : Public
IPv4Connectivity : Internet
IPv6Connectivity : NoTraffic


PS C:\>
Set-NetConnectionProfile -InterfaceIndex 4 -NetworkCategory private
```

Remotezugriff vom Client auf den Server herstellen

Remotedesktopverbindung (`mstsc` – Microsoft Terminal Server Client)

Remotezugriff auf einen Windows-PC

Über das RDP-Protokoll (Remote Desktop Protocol, TCP- und ab Version 8.0 auch UDP-Port 3389) kann eine Terminal-Verbindung zu einem Windows-PC hergestellt werden. Bei der Verbindung zu einem Windows-Rechner ist nur eine Verbindung möglich, bei der ggf. ein angemeldeter Benutzer getrennt wird. Zu einem Windows-Server sind gleichzeitig zwei Verbindungen mit unterschiedlichen Benutzer-Accounts möglich.

Laborübung 04 - DOMAINCONTROLLER, DNS, DHCP

kurz & knapp

- DNS-Grundlagen
- DNS ist in AD integriert
- Aufgaben eines DC

Szenario

Der Windows Server soll als Domaincontroller (Active Directory) mit integriertem DNS arbeiten.

Aufgaben

1. Diskutieren Sie, für welche Aufgaben die Einrichtung von Active Directory auf Domänencontrollern sinnvoll oder erforderlich ist.
2. Installieren Sie, falls noch nicht vorhanden, die Serverrollen Domänencontroller (Active Directory Domänendienste) und DNS (ggf. zuvor Prüfpunkt erstellen).
3. Richten Sie Ihren Windows Server unter folgenden Vorgaben als Domänencontroller ein:
   - Neue Gesamtstruktur
   - DNS-Name der Domäne: z. B. alp10.local
   - NetBIOS-Name der Domäne: z. B. ALP10
   - Übernehmen Sie die Standardeinstellungen für die Speicherorte (Datenbank, Protokoll, …)
   - DNS soll automatisch angelegt werden
4. Überprüfen Sie die Namensauflösung mit nslookup. Testen Sie dabei insbesondere die Namensauflösung und IP-Adressen-Auflösung des Domänencontrollers.

Hinweise

Diskussionspapier

	Lösungen	mit DC möglich	DC erforderlich
Dateiaustausch über das Netzwerk			
Jeder Benutzer hat ein eigenes Homeverzeichnis			
Benutzerverwaltung			
DNS (Namensauflösung)			
DHCP			
Windows (entfernte Installation)			
Windows-Client (Softwareverteilung)			
Windows-Client (Desktopumgebung)			
Windows-Client (Schutz vor Änderungen)			
Internetzugang			
E-Mail			
Antivirenschutz (Windows Defender)			
Client Update (Versionsupdate)			
Client Wiederherstellung (Recovery) Absicherung (mobiler) schuleigener Geräte			

Rollen und Features hinzufügen

Server-Manager – Verwalten – Rollen und Features hinzufügen

Wahl des Domänennamens

Die Endung .local wird im Internet nicht verwendet und kann deshalb keine Kollisionen mit bestehenden Domänen verursachen. Wenn die Schule über einen öffentlichen Domänennamen (z.B. mittelschule-dillingen.de) verfügt, kann es sinnvoll sein, statt .local einen Subdomänen-Namen (z.B. schulnetz.mittelschule-dillingen.de) zu verwenden.

Nachteile der Endung .local

- Es kann kein vertrauenswürdiges SSL-Zertifikat erworben werden.
- Ein lokaler Exchange-Server verwendet standardmäßig Benutzer@Domänennamen. Suffix als Antwortadresse. Emails an diese Adressen (z.B. user@mittelschule-dillingen.local) können nicht zugestellt werden.

nslookup (Name Server Lookup)

Mit nslookup kann ein Nameserver nach der Auflösung eines Namens oder einer IP-Adresse angefragt werden.

```
nslookup <aufzulösende Adresse/aufzulösender Name> <DNS-Server>
```

Wird der DNS-Server nicht angegeben, so wird der in den Netzwerkeinstellungen angegebenen Nameserver befragt.

`nslookup alp.dillingen.de`	Anfrage an den Standard-DNS-Server bezüglich der IP-Adresse von alp.dillingen.de.
`nslookup 194.95.207.10`	Anfrage an den Standard-DNS-Server bezüglich des Rechnernamens für die IP-Adresse 194.95.207.10.
`nslookup alp.dillingen.de www.dillingen.de`	Anfrage an den DNS-Server www.dillingen.de bezüglich der IP-Adresse von alp.dillingen.de.

Antworten von nslookup

`Server: hs16p00.alp130.local`	Name des DNS-Servers, der die Anfrage entgegennimmt.
`Adresse: 192.168.130.10`	IP-Adresse des DNS-Servers, der die Anfrage entgegennimmt.

`Nicht autorisierende Antwort:`	Der angefragte DNS-Server hat die Anfrage nicht selbst beantwortet, sondern an einen anderen DNS-Server weitergeleitet.
`Name: www.alp.dillingen.de`	Name des angefragten Rechners.
`Address(es): 194.95.207.10`	IP-Adresse bzw. IP-Adressen des angefragten Rechners.
`Aliases: alp.dillingen.de`	Weitere Namen des angefragten Rechners.

`ipconfig /displaydns`	Der DNS-Cache wird angezeigt.
`ipconfig /flushdns`	Der DNS-Cache wird geleert.
`ipconfig /registerdns`	Erneuert das DHCP-Lease und die Registrierung des Clients beim DNS-Server.

DNS-Grundlagen

Das DNS ist ein hierarchisch aufgebauter Namensraum für Internetadressen. Grundlegende Informationen finden sich auf den Schulnetzseiten unter .... (siehe PDF)

Domäne bzw. DNS-Domäne

Ein zusammenhängender Teilbereich des DNS-Namensraumes z. B. alp.dillingen.de

Domäne bzw. Windows-Domäne

Lokaler Sicherheitsbereich mit zentraler Verwaltung

FQDN (Full Qualified Domain Name)

Vollständiger Name einer Domäne oder eines Computers im DNS-Namensraum z. B. alp.dillingen.de oder server1.alp.dillingen.de.

Ablauf der Namensauflösung unter Windows

Wird ein Computer über einen Namen angesprochen (z. B. ping pc12), muss der Name in eine IP-Adresse aufgelöst werden. Zur Namensauflösung werden folgende Wege der Reihe nach versucht:

- lokaler Hostname
- lokaler DNS-Cache (incl. hosts-Datei)

- Anfrage an den DNS-Server
- lokaler NetBIOS-Cache
- Anfrage an den WINS-Server
- NetBIOS-Broadcast
- lmhosts-Datei

Weiterführende Informationen

Werkzeuge zur Verwaltung von Domänen

- Active Directory-Benutzer und -Computer (dsa.msc):
  Verwaltung der Benutzer und Computer
- Active Directory-Standorte und -Dienste (dssite.msc):
  Verwaltung der Replikation von Verzeichniseinträgen
- Active Directory-Domänen und -Vertrauensstellungen (domain.msc)
  Verwaltung zusammengehöriger Domänen

Die letzten beiden Verwaltungswerkzeuge sind nur in Strukturen mit mehreren Domänen oder mehreren Standorten nötig.

Sysvol-Freigabe

Die Sysvol-Freigabe ist auf jedem Domänencontroller vorhanden. Der Inhalt dieser Freigabe wird auf allen Domänencontrollern synchron gehalten.

Netlogon-Freigabe

Die Netlogon-Freigabe ist ein Unterverzeichnis von Sysvol und wird damit auch auf allen Domänencontrollern synchron gehalten. Dieses Verzeichnis eignet sich z. B. um Anmeldeskripte zu hinterlegen.

Netzwerkverbindungen zwischen Domänencontrollern

Port 389 TCP/UDP (LDAP)

Port 686 TCP (LDAP SSL)

Port 3268 TCP (Globaler Katalog)

Port 3269 TCP (Globaler Katalog SSL)

Laborübung 05 - DHCP SERVER MIT DER POWERSHELL

kurz & knapp

- Einführung in PowerShell
- DHCP-Dienst
- Ausfallsicherheit

Szenario

Auf dem Domänencontroller soll ein DHCP Server installiert werden.

Aufgaben

1. Installieren Sie auf dem Domänencontroller eine aktuelle Version der Powershell 7 (Download MSI Paket).
2. Passen Sie das Installationsskript an ihre Laborumgebung an und installieren Sie die DHCP Server Rolle!
3. Passen Sie das Konfigurationsskript an Ihre Laborumgebung an und wenden Sie das Skript auf den DHCP Server an.
4. Kontrollieren Sie die vorgenommenen Einstellungen und testen Sie die Funktion des DHCP Servers von einem Client aus.

Weiterführende Aufgaben

5. Installieren Sie auf dem zweiten Domänencontroller ebenfalls die DHCP Server Rolle und konfigurieren Sie ein Fail Over der beiden DHCP Server.
6. Erstellen Sie Reservierungen für die von Ihnen verwendeten Clients.

Hinweise

Installationsskript:

DHCP mit Verwaltungskonsole installieren; Ausrufezeichen taucht auf

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

DHCP Sicherheitsgruppe anlegen mit ausführlicher Meldung

```
Add-DHCPServerSecurityGroup -Verbose
```

DHCP Dienst als konfiguriert kennzeichnen; keine Ausgabe

```
$RegHT = @{
    Path = 'HKLM:\SOFTWARE\Microsoft\ServerManager\Roles\12'
    Name = 'ConfigurationState'
    Value = 2
    }
    Set-ItemProperty @RegHT
```

DHCP autorisieren; keine Ausgabe

```
Add-DhcpServerInDC -DnsName DC01.alp10.local
```

DHCP neu starten

```
Restart-Service -Name DHCPServer –Force
```

Konfigurationsskript:

Konfiguration der DHCP Bereiche

Bereiche festlegen; bitte an eigenes Netzwerk anpassen!

Schuelernetz

```
$SHT01 = @{
    Name = 'Schuelernetz01'
    StartRange = '192.168.10.50'
    EndRange = '192.168.10.99'
    SubnetMask = '255.255.255.0'
    LeaseDuration = '30.00:00:00'
    Delay = '10'
    Type = 'Dhcp'
    Description = 'Standardbereich fuer lokales Schuelernetz01'
    State = 'Active'
    ComputerName = 'DC01.alp10.local'
    }
    Add-DhcpServerV4Scope @SHT01
```


DHCP Serveroptionen konfigurieren

```
$OHT = @{
    ComputerName = 'DC01.alp10.local'
    DnsDomain = 'alp10.local'
    DnsServer = '192.168.10.201'
    Router = '192.168.10.1'
    }
    Set-DhcpServerV4OptionValue @OHT
```

DHCP konfigurieren: Server-Manager – Tools – DHCP

DHCP (Dynamic Host Configuration Protocol)

DHCP ist ein Verfahren, mit dem Computer ihre Netzwerkeinstellungen automatisch zugewiesen bekommen.

Üblicherweise werden folgende Einstellungen mit DHCP übergeben:

- IP-Adresse und Netzwerkmaske
- Gateway
- DNS-Server (Dies muss zwingend der Domänencontroller bzw. der für die Domäne zuständige DNS-Server sein.)

Möglich sind noch weitere Zuweisungen, z. B. WINS-Server, Zeitserver, etc.

DHCP-Kommunikation (DORA)

DHCP-Discover	Der Client sendet eine Anfrage nach einem DHCP-Server.
DHCP-Offer	Der DHCP-Server sendet ein Angebot mit Netzwerkeinstellungen.
DHCP-Request	Der Client fordert die angebotenen Netzwerkeinstellungen vom DHCP-Server.
DHCP-Acknowledge	Der Server bestätigt die Anforderung und reserviert die IP-Adresse.

Die DHCP-Kommunikation zwischen Client und Server findet per Broadcast auf den UDP-Ports 67 und 68 statt.

ipconfig	Anzeige der lokalen IP-Einstellungen
ipconfig /all	Ausführliche Darstellung
ipconfig /release	Freigabe der bestehenden IP-Verbindung
ipconfig /renew	Erneuerung der DHCP-Zuweisung

Laborübung 06 - EINRICHTEN EINER AD-STRUKTUR

Szenario

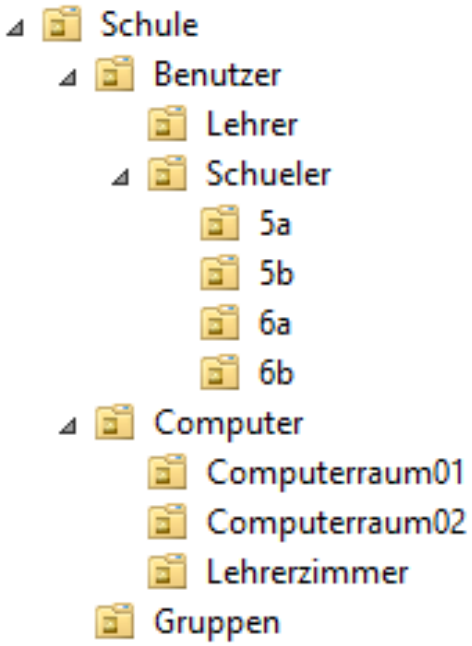
Die vorhandene Schulstruktur soll in der Domäne abgebildet werden.

kurz & knapp

- Rolle von Ous innerhalb von AD
- Gliederungskonzepte im AD
- Geräte und Benutzer in AD aufnehmen

Aufgaben

1. Richten Sie eine AD-Struktur für Ihre Schule nach folgendem Muster ein:



2. Verschieben Sie die bisher angelegten Benutzer in die entsprechenden Organisationseinheiten.
3. Nehmen Sie die Clients in die Domäne auf und verschieben Sie diese ggf. in die entsprechende Organisationseinheit.
4. Legen Sie einen neuen Benutzer an und geben Sie ihm ein gültiges Passwort nach den geltenden Komplexitätsrichtlinien.

Hinweise

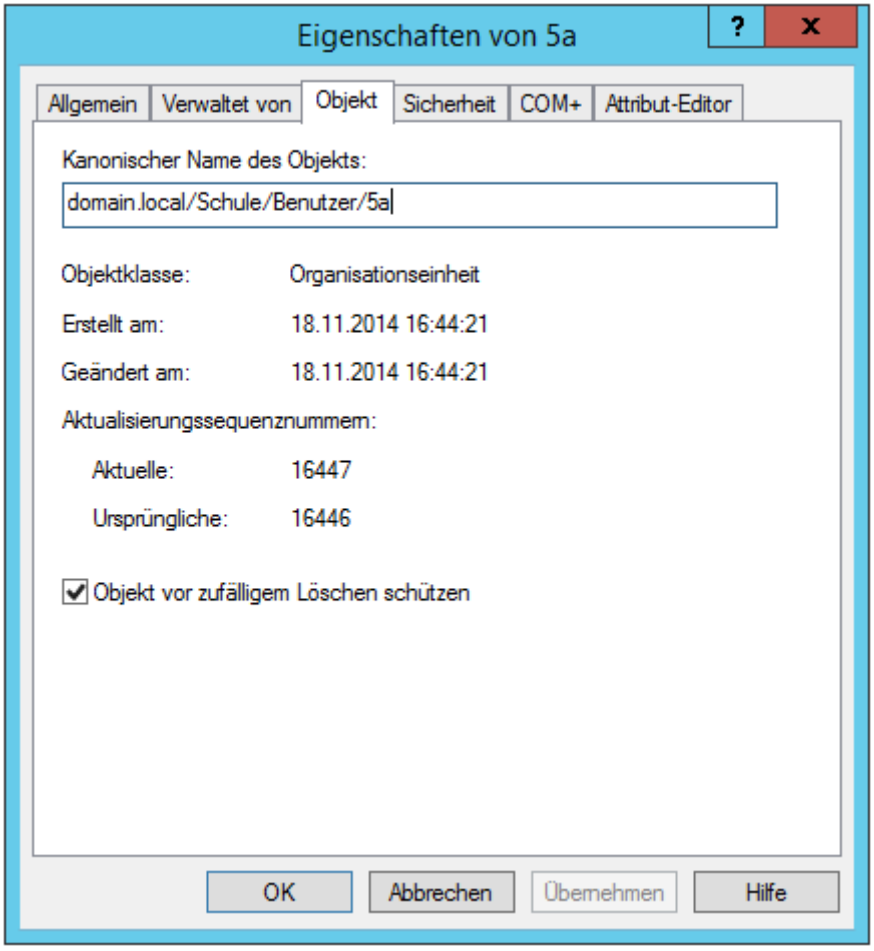
Im Active Directory (Verzeichnisdienst) sind die Rollen und Berechtigungen aller Benutzer und Computer abgebildet. Die spätere Administration wird erleichtert, wenn die Struktur im Active Directory der realen Schulstruktur entspricht.

Client in die Domäne aufnehmen

Computer:	Eigenschaften – Computername – Ändern
Windows-Taste + Pause:	Eigenschaften – Computername – Ändern

OU-Einträge löschen oder verschieben

Beim Anlegen einer Organisationseinheit wird diese standardmäßig vor versehentlichem Löschen geschützt. Soll diese OU nachträglich gelöscht oder verschoben werden, muss bei den Eigenschaften der OU in der Registerkarte Objekt der entsprechende Eintrag deaktiviert werden. Falls die Registerkarte Objekt nicht sichtbar ist, kann diese durch Aktivierung „Erweiterte Features“ im Menüpunkt „Ansicht“ angezeigt werden.



Weiterführende Informationen

Active Directory

Das Active Directory ist eine Datenbank in der Informationen über Benutzer, Gruppen und Computer gespeichert werden. Diese sogenannten Objekte werden in Organisationseinheiten (Organizational Unit, OU) zusammengefasst und verwaltet.

Standardcontainer im Active Directory

Builtin	Vom System vordefinierte Gruppen. Diese können weder gelöscht noch umbenannt oder verschoben werden.
Computers	Computer, die neu in die Domäne aufgenommen werden.
Domain Controllers	Alle Domänencontroller der Domäne.
Managed Service Accounts	Verwaltet z.B. Exchange- oder SQL-Dienstkonten.
Foreign Security Principals	SIDs (Security-IDs) aus anderen Domänen, zu denen eine Vertrauensstellung existiert.
Users	Benutzer und Gruppen, die automatisch angelegt werden.

Mit Ausnahme der Domain Controllers sind die Standardcontainer nicht als Organisatorische Einheiten (OUs) definiert. Deshalb stehen für diese Container bestimmte Funktionen (z. B. Gruppenrichtlinien) nicht zur Verfügung.

Komplexitätsrichtlinien für Passwörter

Wenn die Komplexitätsrichtlinien aktiviert sind, muss ein Passwort Zeichen aus drei verschiedenen Kategorien haben:

Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.

Die Richtlinie kann auch OU basiert zugewiesen werden (PSO).

Laborübung 07 - GRUPPENRICHTLINIEN

kurz & knapp

- Aufbau und Einsatz von GPOs
- (Default)Richtlinien
- GPOs durchsetzen

Szenario

Im EDV-Raum soll die Administration der Clients zentral erfolgen. Einigen Benutzern soll eine eingeschränkte Umgebung präsentiert werden.

Aufgaben

1. Ändern Sie die Kennwortrichtlinie für Domänen so ab, dass auch kurze und einfache Kennwörter erlaubt sind.
2. Erstellen Sie eine Gruppenrichtlinie, die es verbietet, die Systemsteuerung aufzurufen. Lehrkräfte sollen von der Richtlinie nicht betroffen sein. Testen Sie die Funktionalität der Gruppenrichtlinie.
3. Kontrollieren Sie die Telemetrie – und Diagnosedaten, die von den Windows Clients ausgewertet werden.

Hinweise

Die Standard-Domänenrichtlinie

Die Standard-Domänenrichtlinie (Default Domain Policy) ist mit der Domäne verknüpft und wirkt über die Richtlinienvererbung auf alle Benutzer und Computer in der Domäne.

Die Standard-Domänencontrollerrichtlinie

Die Standard-Domänencontrollerrichtlinie (Default Domain Controller Policy) ist mit der Domänencontroller-Organisationseinheit verknüpft, in der standardmäßig die Computerkonten für Domänencontroller gespeichert sind.

Einfache Kennwörter

Default Domain Policy

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Kontorichtlinien – Kennwortrichtlinien

Systemsteuerung verbieten

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Administrative Vorlagen – Systemsteuerung

Aktualisierung der Gruppenrichtlinien

Gruppenrichtlinien werden automatisch alle 90 – 120 Minuten vom Client aktualisiert. Mit dem Befehl gpupdate (am Client) können die Richtlinien sofort aktualisiert werden. Einige Richtlinien wirken erst nach einem Neustart des Computers oder nach dem erneuten Anmelden des Benutzers.

`gpupdate`	Das Gruppenrichtlinienmodul am Client liest neue oder veränderte Richtlinien ein (Group Policy Update).
`gpupdate /force`	Erzwingt, dass alle Gruppenrichtlinien neu gelesen und angewandt werden.

Weiterführende Informationen

Gruppenrichtlinien

Gruppenrichtlinien sind ein Werkzeug, um in einer Active-Directory Domäne Systemeigenschaften, Sicherheitseinstellungen oder Profileigenschaften zu definieren.

Gruppenrichtlinien werden auf Organisationseinheiten vergeben und wirken auf alle Benutzer und Computer in dieser Organisationseinheit.

Hierarchie der Gruppenrichtlinien

In Domänenstrukturen sind Gruppenrichtlinien hierarchisch geordnet. Die Verarbeitung erfolgt in einer bestimmten Reihenfolge:

- Lokale Sicherheitseinstellungen und lokale Gruppenrichtlinien
- Domänen-Gruppenrichtlinien

- Gruppenrichtlinien der Organisationseinheit, von der übergeordneten zur untergeordneten Organisationseinheit.

Wird eine Richtlinie in mehreren Ebenen mit unterschiedlichen Einstellungen aktiviert, dann setzt sich die zuletzt abgearbeitete Richtlinie (OU-Richtlinie) durch.

Ausnahmen der Hierarchie

- Eine Richtlinie kann erzwungen werden und kann damit nicht mehr durch eine nachgeordnete Richtlinie überschrieben werden.
- Bestimmte Richtlinien wirken nur, wenn sie auf Domänenebene (Default Domain Policy) vergeben werden (z. B. Kennwortrichtlinien).

Speicherort der Gruppenrichtlinien

Gruppenrichtlinien werden auf dem Domänencontroller im freigegebenen Verzeichnis SYSVOL unter <Domäne>\Policies gespeichert.

Kontrolle der Gruppenrichtlinien

Am Client:	rsop.msc (Resultant Set of Policies, Richtlinienergebnissatz)
	gpresult.exe /r
Am Server:	Gruppenrichtlinienverwaltung – Gruppenrichtlinienmodellierung Simulation eines Szenarios anhand der Zugehörigkeit eines Computers oder Benutzers zu einer Organisationseinheit (OU).
	Gruppenrichtlinienverwaltung – Gruppenrichtlinienergebnisse Darstellung der tatsächlich auf einen Computer oder Benutzer wirkenden Gruppenrichtlinien.

Bedingungen für Gruppenrichtlinien

Gruppenrichtlinien können von bestimmten Bedingungen, die an Attribute aus dem Active Directory gebunden sind, abhängig gemacht werden. So lässt sich z. B. eine Gruppenrichtlinie für Benutzer erstellen, die nur dann abgearbeitet wird, wenn der Benutzer einer bestimmten Sicherheitsgruppe angehört.

Weitere Beispiele für Gruppenrichtlinien

Letzten Anmeldenamen nicht anzeigen

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Lokale Richtlinien – Sicherheitsoptionen – „Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen“

Beim Anmelden auf Netzwerk warten

Unter Windows wird der Windows-Explorer vor dem Netzwerk geladen. Desktopeinstellungen, die mit Gruppenrichtlinien festgelegt wurden, können daher nicht übernommen werden. Der Computer arbeitet mit den "Cached Logon Credentials". Auch die Softwareverteilung gelingt nur mit der Einstellung:

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Administrative Vorlagen – System – Anmelden – "Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten".

Zugriff auf Teile der Systemsteuerungselemente regeln

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Administrative Vorlagen – Systemsteuerung

Regelmäßige Änderung des Computerkennworts verhindern

Standardmäßig ändert ein Computer ca. alle 30 Tage das Kennwort mit dem er sich beim Domänencontroller authentifiziert. Dies kann zu Problemen führen, wenn der Computer mit einem Festplattenschutz arbeitet oder ein vorheriges Image zurück gespielt wird.

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Lokale Richtlinien – Sicherheitsoptionen – „Domänenmitglied: Änderungen von Computerkennwörtern deaktivieren“

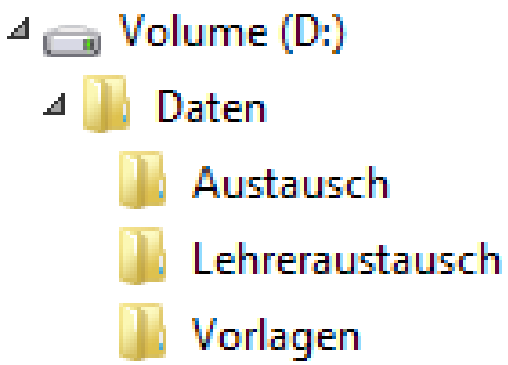
Laborübung 08 - SMB-ZUGRIFF UND NTFS-RECHTE

kurz & knapp

- NTFS und SMB-Rechte
- Freigabekonzept
- Praxisbeispiele

Szenario

Schüler und Lehrer sollen den Server zur Datenablage und zum Austausch von Dateien nutzen. Im Ordner Austausch sollen alle Benutzer Daten ablegen, austauschen und löschen können. Im Ordner Vorlagen stellen Lehrkräfte den Schülern Unterrichtsmaterial zur Verfügung.



Aufgaben

1. Legen Sie auf dem Server zwei Gruppen z. B. Schueler und Lehrer an und ordnen Sie die Benutzer s1, s2, l1, l2 diesen Gruppen zu.
2. Erstellen Sie auf dem Server die angegebene Ordnerstruktur und geben Sie den Ordner *Daten* frei.
3. Im Austauschordner sollen die Schüler und Lehrkräfte lesenden und schreibenden Zugriff haben. Im Vorlagenordner können Schüler lesen, Lehrkräfte lesen und schreiben.
4. Greifen Sie vom Arbeitsplatzcomputer mit unterschiedlichen (auch lokalen) Benutzeraccounts und mit unterschiedlichen Werkzeugen auf die Freigabe am Server zu.
5. Die Freigabe soll über einen Laufwerksbuchstaben angesprochen werden.

Weiterführende Aufgaben

Die angelegte Ordnerstruktur soll gegen versehentliche oder absichtliche Veränderungen geschützt werden.

6. Im freigegebenen Ordner *Daten* soll ein Benutzer keine weiteren Ordner oder Dateien anlegen können.
7. Überprüfen Sie, ob ein Schüler oder eine Lehrkraft in der Lage ist, das Austauschverzeichnis versehentlich zu löschen und verhindern Sie dies gegebenenfalls.
8. Im Vorlagenordner sollen die Lehrkräfte ihre Daten nur in selbst erstellten Ordnern ablegen können. Die Lehrkräfte sollen sich die Daten gegenseitig nicht überschreiben oder löschen können. Schüler und Lehrer können lesend auf alle Dateien zugreifen.
9. Auf den Ordner Lehreraustausch sollen Schüler keinen Zugriff haben. Sorgen Sie dafür, dass die Schüler diesen Ordner nicht sehen.

Hinweise

NTFS (New Technology File System) ist ein proprietäres Dateisystem von Microsoft für alle seine Betriebssysteme. Es bietet einen gezielten Zugriffsschutz auf Dateiebene. Zudem ist im Gegensatz zum veralteten FAT-Dateisystem die Dateigröße nicht auf 4 GB beschränkt.

Windows ermöglicht es, NTFS-Rechte sehr differenziert zu vergeben. In den meisten Fällen genügt es jedoch, Leserechte, Lese-/Schreibrechte und Vollzugriff zu unterscheiden.

Leserecht

Als Leserecht werden die NTFS-Rechte Lesen, Ausführen, Ordnerinhalt auflisten, Lesen zusammengefasst.

Lese-/Schreibrecht

Beim Lese-/Schreibrecht kommen noch zusätzlich die Rechte Ändern und Schreiben hinzu.

Vollzugriff

Der Vollzugriff beinhaltet das Lese-/Schreibrecht. Zusätzlich beinhaltet er noch das Recht Rechte zu vergeben und den Besitz von Dateien zu übernehmen.

Ordner ohne Berechtigungen ausblenden

Server-Manager – Datei-/Speicherdienste – Freigaben - <Freigabe>-Eigenschaften – Einstellungen – Zugriffsbasierte Aufzählung aktivieren

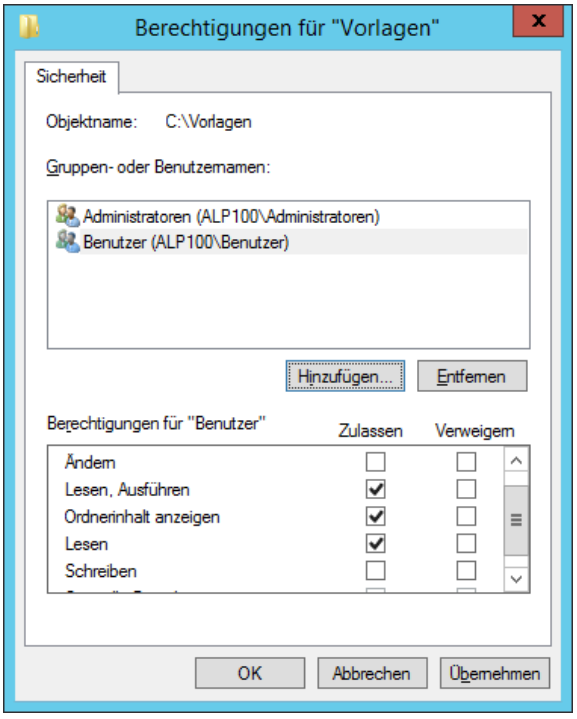
Gruppenrichtlinie zur Laufwerkszuordnung

Gruppenrichtlinie: Benutzerkonfiguration – Einstellungen – Windows-Einstellungen – Laufwerkszuordnungen

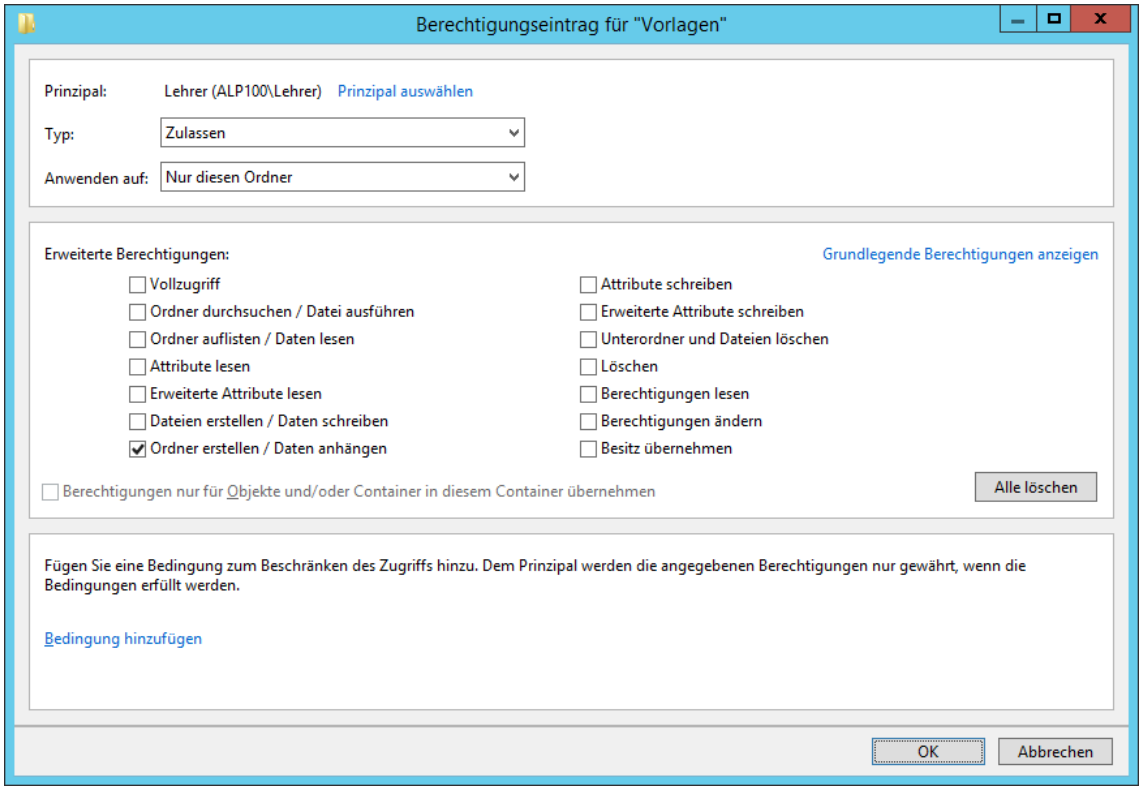
Beispiel für die Vergabe von NTFS-Rechten

Im Vorlagenordner sollen die Lehrkräfte ihre Daten nur in selbst erstellten Ordnern ablegen können. Die Lehrkräfte sollen sich die Daten gegenseitig nicht überschreiben oder löschen können. Schüler und Lehrer können lesend auf alle Dateien zugreifen.

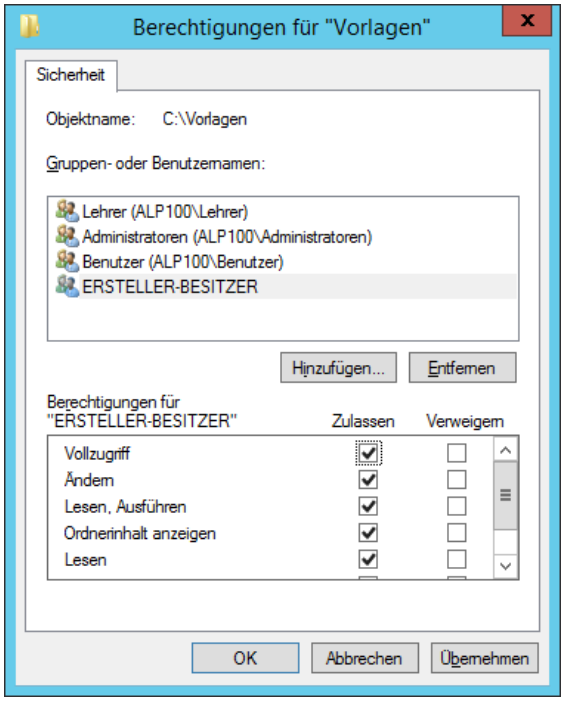
Im ersten Schritt wird für den Ordner Vorlagen die Vererbung unterbrochen und überflüssige Berechtigungen entfernt. Die Gruppe der Administratoren erhält weiterhin Vollzugriff. Die Gruppe der Benutzer erhält Leserechte. Alle Lehrer und Schüler sind in der Gruppe Benutzer enthalten.



Im zweiten Schritt wird der Gruppe Lehrer die Berechtigung gegeben, im Ordner Vorlagen Ordner zu erstellen. Damit können Lehrkräfte Ordner anlegen; sie können den Ordner jedoch nicht umbenennen und auch keine Dateien in diesen Ordner ablegen.



Im dritten Schritt wird der Gruppe „Ersteller-Besitzer“ Vollzugriff gegeben. Hat ein Lehrer einen Ordner angelegt, ist er „Ersteller-Besitzer“ dieses Ordners und hat damit Vollzugriff. Alle anderen Benutzer haben durch die Vererbung Leserechte.



Weiterführende Informationen

Zusammenspiel zwischen Freigaben und NTFS-Rechten

Um über das SMB- bzw. CIFS-Protokoll auf einen Windows-Server zugreifen zu können, ist eine Freigabe am Windows-Server notwendig. Diese Freigabe ist das Eingangstor zum Server.

Die Freigabe kann mit bestimmten Rechten für verschiedene Benutzer versehen werden (Freigabeberechtigungen). Diese Freigabeberechtigungen stellen die maximalen Rechte dar, die ein Benutzer haben kann, wenn er auf diesem Weg auf den Server zugreift. Durch die NTFS-Rechte können die Rechte eines Benutzers weiter eingeschränkt sein.

Eine gebräuchliche Praxis ist es, Freigaben mit den Freigabeberechtigungen „Jeder – Vollzugriff“ oder „Jeder – Ändern“ zu versehen. Die eigentlichen Beschränkungen für einen Benutzer erfolgen über die NTFS-Rechte (Sicherheitseinstellungen).

Zugriff auf administrative Freigaben

Alle Festplattenlaufwerke sind standardmäßig mit einer administrativen Freigabe versehen (C$, D$, …). Das Windows-Verzeichnis ist standardmäßig mit der administrativen Freigaben ADMIN$ verbunden. Der Zugriff auf die administrativen Freigaben kann nur durch einen Eingriff in die Registry dauerhaft unterbunden werden.

`\\Server\C$` Zugriff auf ein Laufwerk

`\\Server\ADMIN$` Zugriff auf das Windows-Verzeichnis

Anlegen versteckter Freigaben

Versteckte Freigaben sind Freigaben, die in der Netzwerkumgebung nicht angezeigt werden. Der Benutzer muss den Freigabenamen kennen, um darauf zuzugreifen.

Versteckte Freigaben unterscheiden sich beim Anlegen von normalen Freigaben nur dadurch, dass am Ende des Freigabenamens das $-Zeichen angehängt wird.

Laborübung 09 - DAS PERSÖNLICHE HOMEVERZEICHNIS

kurz & knapp

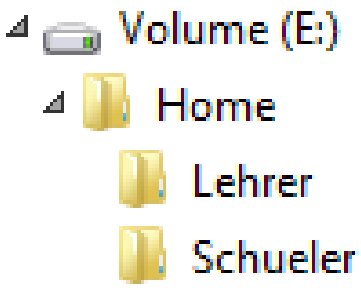
- Basisverzeichnisse
- Rechtekonzepte
- Systemverzeichnisse

Szenario

Jeder Schüler und jede Lehrkraft soll eine persönliche Datenablage im Netzwerk zur Verfügung haben und dieses im Windows-Explorer stets als verbundenes Netzlaufwerk vorfinden.

Aufgaben

1. Erstellen Sie eine Freigabe *Home* und legen Sie die Unterordner *Lehrer* und *Schueler* an.



2. Weisen Sie jedem Schüler und jeder Lehrkraft im dazugehörigen Benutzerprofil ein Homeverzeichnis (Basisverzeichnis) zu.
3. Vergeben Sie die NTFS-Rechte so, dass Schüler keinen Zugriff auf andere Homeverzeichnisse haben. Lehrer sollen Einblick in die Homeverzeichnisse aller Schüler haben.
4. Sorgen Sie dafür, dass beim Speichern unter Dokumente das Homeverzeichnis der Benutzer verwendet wird.

Hinweise

Basisverzeichnis im Benutzerprofil zuweisen

Im Profil des Benutzers wird der Pfad zum Homeverzeichnis einem Laufwerksbuchstaben zugeordnet. Das Homeverzeichnis wird dadurch automatisch angelegt und bei der nächsten Anmeldung des Benutzers mit dem Laufwerksbuchstaben verknüpft. Die Rechte des Benutzers werden vom System automatisch so gesetzt, dass dieser Vollzugriff hat.

Basisordner:

```
H:    \\server\Freigabe\Ordner\%username%
```

Ordner Dokumente umleiten

Der Ordner „Dokumente“ ist im Benutzerprofil gespeichert. Damit Dokumente standardmäßig auf dem Server gespeichert werden, sollte der Ordner „Dokumente“ in das Homeverzeichnis des Benutzers umgeleitet werden.

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Windows-Einstellungen – Ordnerumleitung

Soll der Administrator Zugriff auf den Ordner „Dokumente“ erhalten, dürfen dem Benutzer keine exklusiven Zugriffsrechte gewährt werden.

Damit die Gruppenrichtlinie für die Ordnerumleitung erfolgreich wirken kann, muss für die Freigabeberechtigung Vollzugriff gewährt werden.

Die Ordnerumleitungen für Bilder, Videos und Musik können so festgelegt werden, dass sie dem Ordner „Dokumente“ folgen.

Die Funktion „Ordner umleiten“ wird von Microsoft nicht aktiv weiterentwickelt. Zum Testen sollte ein Benutzer verwendet werden, der an dem lokalen PC noch nicht angemeldet war.

Laborübung 10 - SOFTWAREVERTEILUNG ÜBER GRUPPENRICHTLINIEN

Steht für eine Software ein MSI-Paket (Microsoft Software Installation) zur Verfügung, so kann die Software innerhalb der Domäne verteilt werden. Das MSI-Paket muss über eine Freigabe zur Verfügung gestellt werden.

kurz & knapp

- MSI und MSIX Pakete
- Konzept deprecated
- Ersteinrichtung

Zuweisung eines MSI-Paketes über Gruppenrichtlinien

Gruppenrichtlinie: Computer- oder Benutzerkonfiguration – Richtlinien – Sofwareeinstellungen – Softwareinstallation

MSI-Paket über den Netzwerkpfad auswählen (kein lokaler Pfad).

Erweiterte Einstellungen

„Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt."

Wird der Anwender oder der Computer aus der Zuständigkeit der Gruppenrichtlinie entfernt, so wird die Software deinstalliert.

Beim Neustart auf das Netzwerk warten

Die Softwareverteilung gelingt nur, wenn vor dem Start des Installationsvorganges das Netzwerk zur Verfügung steht.

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Administrative Vorlagen – System – Anmeldung: „Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten".

Mit erhöhten Rechten installieren

Bei der Zuweisung eines MSI-Paketes für eine bestimmte Benutzerkonfiguration kann es erforderlich sein, dem MSI-Paket zur Installation erhöhte Rechte zuzuweisen, da die normalen Benutzerrechte nicht ausreichen.

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Administrative Vorlagen – Windows-Komponenten – Windows Installer: „Immer mit erhöhten Rechten installieren"

Beispiel: Chrome Browser

Der Chrome-Browser von Google lässt sich in der „Chrome for Business“ -Edition im Windows Domänen-Netzwerk per Gruppenrichtlinie verteilen und verwalten.

Vorbereitungen

- Google Chrome for Business als MSI-Installer herunterladen und auf einer Netzwerkfreigabe speichern.
- Die Richtlinienvorlagen herunterladen und entpacken.
- Die Dateien “chrome.admx” nach “C:\Windows\PolicyDefinitions” kopieren.
- Die deutsche “chrome.adml” nach “C:\Windows\PolicyDefinitions\de-DE” kopieren.

Die Vorlagendateien können auch in der Gruppenrichtlinienverwaltung importiert werden.

Google Chrome per Gruppenrichtlinie verteilen

- Die Gruppenrichtlinienverwaltung öffnen.
- Ein neues Gruppenrichtlinienobjekt anlegen und bearbeiten.
- Zu “Computer- oder Benutzerkonfiguration – Richtlinien – Softwareinstallation” wechseln.
- “Aktion – Neu – Paket…” anklicken.
- Den MSI-Installer auswählen. Achtung: Nicht via lokalen Pfad, sondern via UNC auswählen. Andernfalls schlägt die Verteilung fehl!
- Im Dialog “Software bereitstellen” “Zugewiesen” auswählen.
- Das Gruppenrichtlinienobjekt mit der Domäne oder Organisationseinheit verknüpfen.

Je nachdem ob die Softwareinstallation auf Computer oder Benutzer angewendet wird, wird der Browser beim nächsten Start des Computers oder bei der nächsten Benutzeranmeldung installiert.

Laborübung 11 - DRUCKEN IM NETZWERK

kurz & knapp

- Druckdienste
- Drucken über Serverfreigaben
- Standarddrucker

Szenario

Jeder Computerraum verfügt über einen eigenen Drucker. Die Benutzer sollen standardmäßig die Drucker im jeweiligen Raum nutzen können. Ungewollte Ausdrucke sollen möglichst vermieden werden.

Aufgaben

1. Die Benutzer sollen automatisch den Drucker im jeweiligen Raum als Standarddrucker zur Verfügung haben.

Hinweise auf Installationskonzepte für das Drucken

Lokale Installation am Client

Am einfachsten ist es, wenn alle Drucker lokal auf den Clients installiert sind. Die Benutzer wählen je nach Standort den richtigen Drucker aus.

In der Praxis kann dies so funktionieren, dass im vorbereiteten Image für die Clients alle Drucker aller Räume installiert sind.

Als Standard-Drucker ist ein PDF - Drucker ausgewählt.

Durch die Netzwerkinfrastruktur (VLANs, Firewall) wird verhindert, dass Drucker anderer Räume angesprochen werden.

Installation eines Netzwerkdruckers am Client (Lokaler Drucker)

Systemsteuerung – Geräte und Drucker – Drucker hinzufügen – Lokalen Drucker oder Netzwerkdrucker mit manuellen Einstellungen hinzufügen

Drucken über eine Freigabe eines Servers

Der Drucker wird am Server installiert und freigegeben. Die Clients greifen über die Freigabe am Server auf den Drucker zu. Bei diesem Verfahren kann der Server die Druckertreiber für die Clients bereitstellen.

Installation und Freigabe eines Netzwerkdruckers am Server

Systemsteuerung – Geräte und Drucker – Drucker hinzufügen – IP Adresse – Treiber wählen – Freigabename festlegen – im Verzeichnis auflisten

Zuweisen eines Druckers am Client

1. Durch den angemeldeten Benutzer (Rechtsklick auf die Freigabe)
2. Durch Gruppenrichtlinien
3. Durch Anmeldeskripte

Druckerzuweisung durch Gruppenrichtlinien

Mit Gruppenrichtlinien können Drucker sowohl benutzer- als auch computerabhängig zugewiesen werden. Empfohlen werden dabei Druckertreiber vom Typ 4.

Drucker nach Raumzugehörigkeit zuweisen

Neue Rolle am DC:	Installieren der Rolle „Druck- und Dokumentendienste“
Druckverwaltung:	Server – Treiberpakete hinzufügen
Druckverwaltung:	Drucker – neuen Drucker hinzufügen, freigeben
Gruppenrichtlinie:	Erstellen einer Gruppenrichtlinie zur Verteilung der Drucker und Zuweisen dieser Richtlinie auf die betreffenden OUs
Drucker rechte Maus:	„Mit Gruppenrichtlinie bereitstellen“, zuvor erstellte Gruppenrichtlinie auswählen

Druckerzuweisung per Computerrichtlinie

Gruppenrichtlinie:	Computerkonfiguration – Einstellungen – Systemsteuerungseinstellungen – Drucker Neu – TCP/IP Drucker

Druckerzuweisung per Benutzerrichtlinie

Gruppenrichtlinie:	Benutzerkonfiguration – Einstellungen – Systemsteuerungseinstellungen – Drucker Neu – freigegebener Drucker

Druckerinstallation soll ohne administrativen Eingriff erfolgen (Point and Print)

Bei Windows ab Version 7 verhindert diese Richtlinie, dass bei den Clients evtl. eine Warnung oder eine Eingabeaufforderung mit erhöhten Rechten erscheint, um den Drucker zu installieren.

Gruppenrichtlinie:	Computerkonfiguration – Richtlinien – Administrative Vorlagen – Drucker – „Point-and-Print-Einschränkungen“ – deaktivieren

Notizen

Laborübung 12 - SKRIPTE

kurz & knapp

- Freigabeverzeichnisse
- Druckerzuweisung
- Start/Stop Skripte

Szenario

Jedem Schüler und jeder Lehrkraft soll über ein Anmeldeskript ein komfortabler Datenzugriff und eine passende Umgebung bereitgestellt werden. Alle Netzlaufwerke sollen über Laufwerksbuchstaben angesprochen und Drucker sollen den Benutzern automatisch zugewiesen werden. Beim Start und beim Beenden des Computers können vorbereitete Services und Dienste gestartet werden.

Aufgaben

1. Erstellen Sie ein Anmeldeskript, so dass die Benutzer alle für sie interessanten Freigaben am Server über Laufwerksbuchstaben ansprechen können.
2. Die Mitglieder der Gruppe Schuelerzeitung sollen ein eigenes Projektverzeichnis bekommen, das über den Laufwerksbuchstaben S: angesprochen wird.
3. Variieren Sie die Zuweisung des Anmeldeskripts

   - über das Benutzerprofil
   - über eine Gruppenrichtlinie

Hinweise

Verbinden einer Freigabe mit einem Laufwerk

```
net use Laufwerk: \\server\freigabe
net use x: \\192.168.130.10\Daten
net use x: \\Server\Daten
```

Zuweisung eines Login-Skriptes im Benutzerprofil

Damit das erstellte Login-Skript vom System verwendet wird, muss es in der Netlogon-Freigabe gespeichert sein. Im Profil des Benutzers wird lediglich der Dateiname des Skriptes eingetragen, da das System automatisch auf die Netlogon-Freigabe zugreift. Es können folgende Dateitypen verwendet werden: .bat, .cmd, .vbs, .com oder .exe.

Zuweisung eines Login-Skriptes über Gruppenrichtlinien

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Windows-Einstellungen – Skripts – Anmelden – Dateien anzeigen – Hinzufügen

Windows schlägt als Speicherort für Anmeldeskripte, die über Gruppenrichtlinien zugewiesen werden, das Gruppenrichtlinienverzeichnis vor. Damit wird das Skript zusammen mit der Gruppenrichtlinie gespeichert. Nachteilig daran ist, dass die Skripte nicht alle zentral an einer Stelle liegen. Alternativ kann deshalb auch der Netlogon-Pfad des Anmeldeservers angegeben werden: %Logonserver%\netlogon\<Skript>

Anmeldeskript sichtbar ausführen

In der Testphase ist es sinnvoll, das Anmeldeskript sichtbar ausführen zu lassen.

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Administrative Vorlagen – System – Skripts:

- Anmeldeskript gleichzeitig ausführen
- Anmeldeskript sichtbar ausführen

Weiterführende Informationen

Reihenfolge beim Abarbeiten von Login-Skripten

1. Login-Skripte über Gruppenrichtlinien
2. Laufwerksverbindungen auf lokaler Ebene
3. Login-Skript, dessen Pfad im Active-Directory-Profil des Benutzers hinterlegt ist.

Anmeldeskripte

Anmeldeskripte oder Loginskripte sind neben den Gruppenrichtlinien ein zentrales Steuerungselement, um Benutzern eine spezifische Umgebung bereitzustellen.

Skripte können in folgenden Situationen ausgeführt werden:

- Beim Starten oder Herunterfahren eines Computers
- Beim Anmelden oder Abmelden eines Benutzers

Beispiele für Anmeldeskripte

Zuweisung eines Laufwerksbuchstabens

```
@echo off
REM Zuweisen einer Laufwerksverbindung;
REM Vor der Verbindung wird das Laufwerk sicherheitshalber getrennt.

net use x: /delete 2>nul
net use x: %logonserver%\Daten /persistent:no
```

Zuweisung eines Laufwerks in Abhängigkeit der Gruppenmitgliedschaft

```
@echo off
REM Zuweisen einer Laufwerksverbindung
REM in Abhängigkeit der Gruppenmitgliedschaft
net user /DOMAIN %username% | find „G_Schuelerzeitung“
if not errorlevel = 1 (
   net use s: %logonserver%\Schuelerzeitung /persistent:no
)
```

Weitere (Power Shell) Skripte als Beispiele

finden sich auf der SCHULNETZ Webseite unter weiterführende Informationen

Skript Editoren

AutoIT: https://www.autoitscript.com/site/

KiXtart: http://www.kixtart.org/

ERGÄNZENDE ÜBUNGEN

Laborübung 13 - UPDATE EINES DOMÄNENCONTROLLERS

kurz & knapp

- FSMO Rollen
- Update Strategie
- Virtualisierung

Szenario

Ein bestehender Domänencontroller z.B. auf Basis von Server 2003 oder 2008, soll auf einen Domänencontroller auf Basis von Server 2012 R2 upgedatet werden.

Ein bestehender Domänencontroller soll auf eine neue Hardware umgezogen und ggf. virtualisiert werden.

Update eines Domänencontrollers

Nicht empfohlene Vorgehensweise: Sukzessive Migration von Server 2003 auf Server 2008, Server 2008 R2, Server 2012, Server 2012 R2 usw. bis Server 2022.

Gründe:

- Migration von 32-Bit-Versionen auf 64-Bit-Versionen nicht möglich
- Veraltete Hardware bleibt bestehen
- Jeder Migrationsschritt kann scheitern (Backup notwendig)

Empfohlene Vorgehensweise:

Ein zweiter Domänencontroller mit aktuellem Serverbetriebssystem wird in die bestehende Domäne als weiterer Domänencontroller aufgenommen. Anschließend wird der bisherige DC zu einem normalen Server herabgestuft. Die FSMO-Rollen werden automatisch auf den neuen DC übertragen. Der neue Domänencontroller ist gleichzeitig auch der neue DNS-Server. Dies muss den Clients bzw. dem DHCP-Server mitgeteilt werden.

Dienste und Speicherbereiche, die auf dem ehemaligen DC noch aktiv sind (z. B. DHCP, Druckdienste, Dateifreigaben, Homeverzeichnisse, etc.) müssen manuell verschoben werden. Anschließend kann der herabgestufte Server aus der Domäne genommen und abgeschaltet werden.

Betriebsmasterfunktionen und FSMO-Rollen

Die Active-Directory-Datenbank wird zwischen allen Domänencontrollern einer Domäne synchronisiert. Man erhält dadurch eine gewisse Redundanz und Sicherheit. Bestimmte Funktionen dürfen in einer Domäne jedoch nur einmal vorhanden sein.

Auch in einer Gesamtstruktur mit mehreren Domänen müssen bestimmte Aufgaben (z. B. Benennung von Domänen) von einer einzigen Stelle kontrolliert werden.

Insgesamt gibt es fünf Rollen, die lediglich auf einem Domänencontroller laufen. Diese FSMO-Rollen (Flexible Single Master of Operation) oder Betriebsmaster-Funktionen müssen ggf. vor dem Austausch eines Domänencontrollers auf einen anderen Domänencontroller übertragen werden.

FSMO-Rollen in der Gesamtstruktur

Domänennamen-Master
: Kontrolliert das Hinzufügen, Entfernen oder Umbenennen von Domänen in der Gesamtstruktur.

Schema-Master
: Im Schema sind alle Objekte und Attribute definiert, die im Active-Directory vorkommen können. Jede Active-Directory-Gesamtstruktur hat nur ein Schema. Der Schema-Master kontrolliert Änderungen im Active Directory-Schema.

FSMO-Rollen in einer Domäne

PDC-Emulator
: In Domänen mit NT4 Backup-Domänencontrollern (BDCs) fungiert der PDC-Emulator als Primary Domain-Controller. Darüber hinaus ist er für die Aktualisierung von Kennwortänderungen, für die Durchsetzung von Gruppenrichtlinien und für die Zeitsynchronisation erforderlich.

RID-Master
: In einer Domäne ist jedem AD-Objekt eine eindeutige SID (Security-ID) zugeordnet, die aus der Domänen-ID und einer relativen ID (RID) besteht. Die RIDs werden den Domänencontrollern in Blöcken von ca. 500 Stück zur Verfügung gestellt. Ein Domänencontroller kann nur so lange neue Objekte anlegen bis alle RIDs verbraucht sind.

Infrastrukturmaster
: Der Infrastrukturmaster verwaltet den Globalen Katalog (Suchindex über alle ADs in der Gesamtstruktur). Er ist für die Aktualisierung von Verweisen von Objekten innerhalb der Domäne und zu Objekten in anderen Domänen verantwortlich. In Strukturen

mit nur einer Domäne spielt der Infrastrukturmaster praktisch keine Rolle.

`netdom query fsmo`	Zeigt an, auf welchen Servern die Betriebsmaster-rollen aktiviert sind.
`dsquery server -hasfsmo pdc`	Zeigt alle Rollen einzeln an (Statt pdc ist auch rid, infr, schema und name möglich)

Notizen

Laborübung 14 - ANLEGEN VON BENUTZERN

kurz & knapp

- Bulkimport aus CSV Datei
- PowerShell
- AD Struktur und Benutzer

Szenario

Aus der Schülerdatei soll eine Schülerliste exportiert und im Active Directory eingelesen werden. Accounts, die noch nicht existieren, sollen neu angelegt werden, bereits existierende Accounts sollen gegebenenfalls in die richtige Klasse verschoben werden.

Einrichten der AD-Struktur mit Skripten

Powershell 5.2 ist ein Bestandteil der Windows Server 2019/22 Installation. Eine neuere Version 7.x kann direkt von Microsoft heruntergeladen und installiert werden. Die verfügbaren Befehle mit denen man das AD bearbeiten kann sind dokumentiert.

Get-Command Get-Ad*

Listet alle AD Befehle auf, mit denen man das AD abfragen kann.

Get-Command Set-AD*

Listet alle Befehle auf, mit denen man das AD bearbeiten kann.

Üblicherweise bearbeitet man das AD nicht direkt von einem Domänencontroller aus. Skripte aus unbekannten Quellen können ein Sicherheitsrisiko darstellen.

Set-ExecutionPolicy -ExecutionPolicy Undefined -Scope CurrentUser

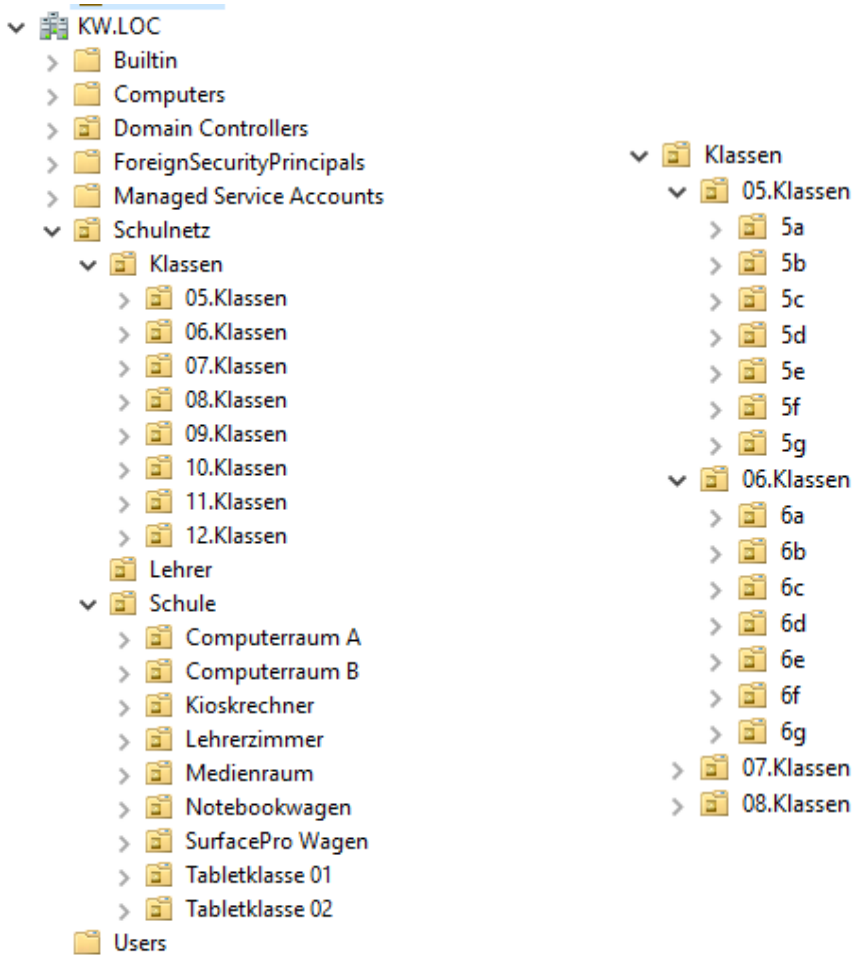
Dieser Befehl ermöglicht es dem aktuell angemeldeten Benutzer, Skripte aus unbekannten Quellen (nicht signiert) auszuführen.

Struktur der OUs

Die bereits vorhandene Struktur wird nicht verwendet. Die beiden Domänenkontrollerkonten sollten in der OU Domain Controllers auftauchen.

Die Schulstruktur wird folgendermaßen modelliert:

- Es gibt eine **OU Schulnetz**. Dies ist der oberste Knoten der Schulstruktur, alles andere liegt unterhalb.
- In der nächsten Ebene gibt es eine **OU Lehrer** (alle Benutzerkonten der Lehrer), eine **OU Schule** (alle Räume und Computerkonten der Schule) und eine **OU Klassen** (alle Klassenstufen bzw. Klassen der Schule). Die Klassen sind aufgeteilt.



Man kann diese Struktur von Hand anlegen. Dabei kann man erstellte OUs nur wieder löschen, wenn man den Schreibschutz (beim Anlegen) entfernt. Die Skripte zum Anlegen der User benötigen diese Struktur.

Die Skripte arbeiten folgende Schritte ab:

- Unsignierte Skripte zulassen
- Klassenstufen und Klassen anlegen: Vorgegeben sind die Klassenstufen 5 bis 12 mit den Klassen a bis g
- Schule anlegen: OUs für Lehrer und alle (Computer)räume der Schule. Die Liste der Räume kann angepasst werden.
- Sicherheitsgruppen anlegen: Alle Benutzer, Alle Lehrer, Alle Schüler
- Lehreraccounts in der OU Lehrer anlegen
- Schüleraccounts in der jeweiligen Klasse anlegen.

Input für die Skripte

Im Beispiel wird als Name der Domäne KW.LOC verwendet. In allen Skripten muss man das an allen Stellen anpassen, wenn man davon abweicht!
Es gibt keine zentrale Variable für den Domänennamen in dieser Version der Skripte.

Die Accounts müssen aus zwei CSV Dateien eingelesen werden, die man am einfachsten in einer Tabellenkalkulation erstellt. Die Daten aus der Schulverwaltung oder digitale Klassenlisten können ein Ausgangspunkt sein.
Die CSV Dateien enthalten 5 Spalten, deren Namen nicht verändert werden darf:

- GivenName
- Surname
- Description
- Company
- Password

In den Spalten GivenName und Surname entfernt das Script alle Umlaute (Anpassung möglich) und geht davon aus, dass in den restlichen Spalten keine Umlaute vorkommen.

Zuordnung für logische Gliederung an der Schule:

Description bei den Schüleraccounts für die Klassenstufe (z.B. 07. Klassen), bei den Lehreraccounts für die Fächer.

Company wird bei den Schüleraccounts als Klasse hinterlegt bzw. bei den Lehreraccounts als Funktionsbezeichnung.

Speicherort der CSV Dateien

Schüleraccounts: C:\tmp\aduser.csv

Lehreraccounts: C:\tmp\lehrer.csv

Arbeitet man nicht lokal, so sollte man hier UNC Freigabepfade verwenden.

Laborübung 15 - ZEITSYNCHRONISATION

In einer Windows-Domäne wird die korrekte Uhrzeit automatisch vom Domänencontroller (Domänencontroller mit der FSMO-Rolle PDC-Emulator) auf die Clients übertragen.

kurz & knapp

- Host PC Zeiteinstellungen
- AD Zeiteinstellung
- Manuelle Synchronisation
- Externe Zeitquellen

Normalerweise sollten an den Zeiteinstellungen keine Änderungen notwendig sein. Bei Problemen, die auf eine abweichende Zeit innerhalb der Domäne zurückzuführen sind, kann folgendes überprüft werden:

- Sind alle Clients und Server in der gleichen Zeitzone?
- Ist die Hardware-Uhr bei den Clients in Ordnung oder kommt es regelmäßig zu Problemen, wenn die Clients längere Zeit nicht in Betrieb waren?
- Ist am Domänencontroller ein funktionierender Zeitserver eingetragen?

Aufgaben

1. Überprüfen Sie am Server die korrekte Zeitzone und die Uhrzeit.
2. Stellen Sie fest, welcher Internet-Zeitserver zur Zeitsynchronisation verwendet wird.
3. Stellen Sie gegebenenfalls am Domänencontroller den Zeitserver ptbtime2.ptb.de als Standard-Zeitserver ein.

Hinweise

Virtualisierte Umgebungen

Läuft der Domänencontroller in einer virtualisierten Umgebung (z. B. Hyper-V), dann wird üblicherweise die Zeit des Host-PC übernommen.

Überprüfung des Zeitserverdienstes

`w32tm /tz`	Zeigt die aktuelle Zeitzone an.
`w32tm /query /source`	Zeigt den aktuell genutzten Zeitserver an.

```
w32tm /config /manualpeerlist:ptbtime2.ptb.de /syncfromflags:manual
```

	Legt den Zeitserver fest, der zukünftig verwendet werden soll.
`w32tm /config /update`	Die Konfigurationsänderung wird angewandt.
`w32tm /resync`	Synchronisiert die Uhrzeit mit dem Zeitserver
`net stop/start w32time`	Der Zeitserverdienst wird beendet/gestartet.
`w32tm /monitor`	Anzeige des Zeitservers in der Domäne und der externen Zeitquelle
`net time /domain:FQDN /set /yes`	Stellt auf dem Client die passende Uhrzeit der Domäne ein

Weiterführende Informationen

Die Clients synchronisieren ihre Uhrzeit bei der Anmeldung an den Domänencontroller automatisch. Weichen die Uhrzeiten zu sehr voneinander ab, ist eine Anmeldung am Domänencontroller nicht möglich. Die Abweichung darf bei standardmäßiger Verwendung des Kerberos Protokolls zur Kommunikation maximal 5 Minuten betragen.

In größeren Strukturen, mit mehreren Domänencontrollern oder Domänen ist die Hierarchie wie die Uhrzeit synchronisiert wird, festgelegt. Üblicherweise synchronisiert sich der erste Domänencontroller mit einer externen Zeitquelle und wirkt als Zeitgeber für die anderen Domänencontroller und Clients.

Festlegung des Zeitservers entsprechend der Domänenhierarchie:

```
w32tm /config /syncfromflags:domhier
```

Anfragen an eine Zeitquelle können im symmetrischen Modus oder im Client-Modus gesendet werden. Im symmetrischen Modus agiert der anfragende Computer als gleichberechtigter Partner und handelt mit dem angefragten Zeitserver eine gemeinsame Zeit aus. Von externen Zeitservern wird dies im Allgemeinen nicht akzeptiert. Im Client-Modus übernimmt der anfragende Computer die vom Zeitserver erhaltene Zeit.

Anfrage im Client-Modus:

```
w32tm /config /manualpeerlist:<server>,0x8 /syncfromflags:manual
```

NTP Network Time Protocol

SNTP Simple Network Time Protocol

Anfragen an den Zeitserver werden über den UDP-Port 123 gesendet. Dieser darf nicht durch eine Firewall blockiert sein.

Laborübung 16 - VERWENDUNG DES ADMINCENTER

kurz & knapp

- Weboberfläche (SSL)
- Mehrere Server
- Brücke zu Azure Diensten

Szenario

Windows Server soll über das Admin Center verwaltet werden

Aufgaben:

1. Installieren Sie Windows Admin Center auf einem Server und/oder auf einem Windows 11 Client.
2. Rufen Sie Windows Admin Center auf und verbinden Sie sich mit dem Windows Server um die Hyper-V Rolle zu administrieren.

Hinweise

Das Windows Admin Center ist ein lokal bereitgestelltes, browserbasiertes Verwaltungstool, das die Verwaltung von mehreren Windows Servern ermöglicht.

Der Zugriff auf Server und von Verwaltungscomputern aus muss mit Zertifikaten abgesichert sein. Selbst signierte Zertifikate laufen nach 60 Tagen ab und müssen dann erneuert werden.

Das Admin Center funktioniert mit den Browsern Google Chrome und Microsoft Edge. Diese Browser müssen auf dem Server bzw. zugreifenden Client installiert sein.

Die Installation auf Domänencontrollern ist nicht möglich.

Wenn im Webbrowser im Windows Admin Center eine Verbindung zu einem Server erfolgt, wird die Verbindung zwischen einem Admin Center Gateway und dem entsprechenden Server hergestellt. Alle Server kommunizieren nur mit diesem Gateway, das seinerseits mit den verwendeten Browsern kommuniziert.

Die Installation kann über den Download des msi Pakets erfolgen:

https://www.microsoft.com/en-us/evalcenter/evaluate-windows-admin-center

Bei der Installation werden Zertifikate verwendet und einige Ports zur Freigabe festgelegt.

Laborübung 17 - WEITERE SERVERDIENSTE UND ROLLEN

Microsoft Windows Server bietet weitere rollenbasierte Dienste im Netzwerk an. Zusätzlich lässt sich die lokale Struktur (On premisses) mit einer Online Struktur verbinden (Hybride Strukturen).

kurz & knapp

- Überblick
- Rollen für Server
- Hybride Strukturen

Windows Backup und Windows Update Services

Seit der Version 2008 steht eine Backupmöglichkeit für Windows Server zur Verfügung.

Windows Update Services vereinfachen das Update und Patch Management im Windows Netzwerk.

Windows Bereitstellungsdienste (WDS)

Windows Deployment Services bieten eine einfache Möglichkeit Windows Images über Netzwerk auf Clients zu installieren. Images können sehr weitreichend angepasst werden; die Installation automatisiert werden (Zero Touch).

AD Connect und AD Federation Services

Eine lokale Windows Domäne kann im Allgemeinen nicht als Identitätsprovider für cloudbasierte Dienste verwendet werden. Um SSO Szenarien zu ermöglichen (z.B. mit Office 365) muss die lokale Struktur mit den Onlinediensten von Microsoft verbunden werden.

MICROSOFT AZURE

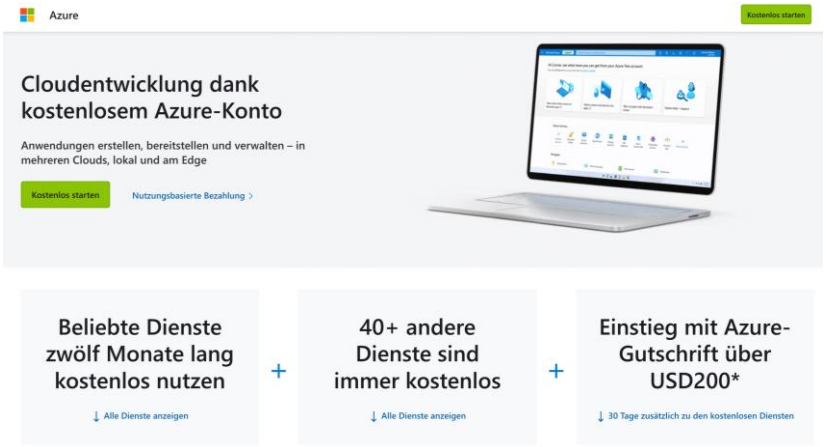
Laborübung 18 - MICROSOFT AZURE PROBEKONTO

kurz & knapp

- IaaS
- PaaS
- Kontotypen

Szenario

Microsofts Clouddienste sollen durch Erstellen einer AD Struktur online erkundet werden. Dazu wird ein Microsoft Azure Konto benötigt.



Aufgaben:

1. Melden Sie sich an der Seite portal.azure.com mit einer neuen E-Mail-Adresse *@outlook.de an. Führen Sie alle Schritte des Anmeldedialogs durch und aktivieren Sie die „FA für das Administratorkonto.
2. Legen Sie eine erste Ressourcengruppe „Schulnetz-PROD“ an und kontrollieren Sie Ihr Anfangsguthaben (200 $).
3. Richten Sie ein weiteres Admin Konto ein sowie einen Netzwerkadministrator und einen Storage-Verwalter.

Hinweise

Azure Tenant

Ein eindeutiger, logischer Platzhalter, unter dessen Kontext alle Ressourcen erstellt und verwaltet werden. Wird der Tenant eingerichtet, so wird bereits eine angepasste AD-Umgebung erstellt. Hier kann optional auch ein DNS-Name verwendet werden.

Aufbau der Organisationsstruktur

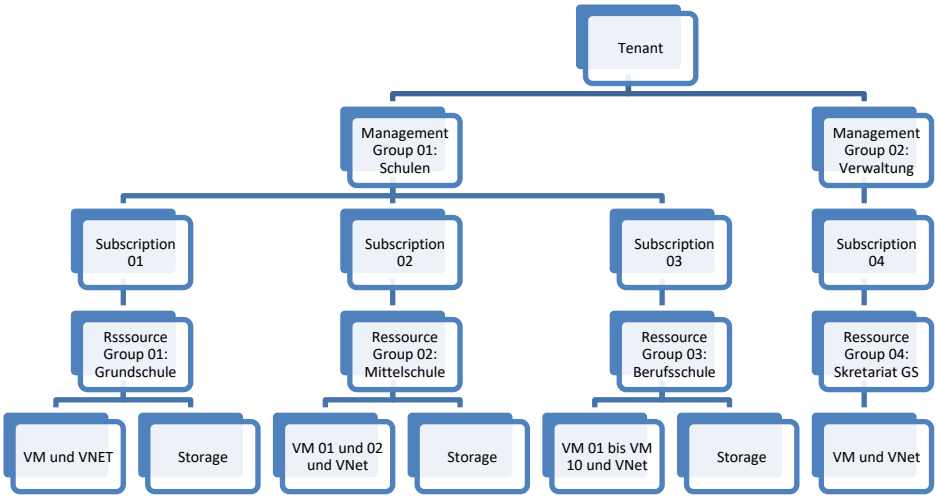
Azure Management Groups (Verwaltungsgruppen) und Subscriptions (Abonnements) organisieren und steuern den gewünschten Aufbau der angelegten Struktur.

Azure Policies

Hier können Compliance Regeln auf verschiedenen Ebenen erstellt und auch überprüft werden. Verschiedene Teile der Struktur können unterschiedliche Anforderungen haben.

RBAC

Role based Access Control regelnd en Zugriff auf Ressourcen und sind unabhängig von Windows Daten – und Zugangsberechtigungen. So kann es sein, dass ein Netzwerkadministrator Subnetze verwalten darf, aber auf die Netzwerke selbst keinen Zugriff hat. Dasselbe gilt für Speicherbereiche in der Azure Cloud.



Azure Verfügbarkeit

Mehrere physische Rechenzentren sind einem logischen Bereich (Region) zugeordnet. Diese Rechenzentren einer Region sind mit dedizierten Leitungen (geringe Latenz) miteinander verbunden. Die Auswahl der Region beeinflusst die Hochverfügbarkeit einer Ressource.

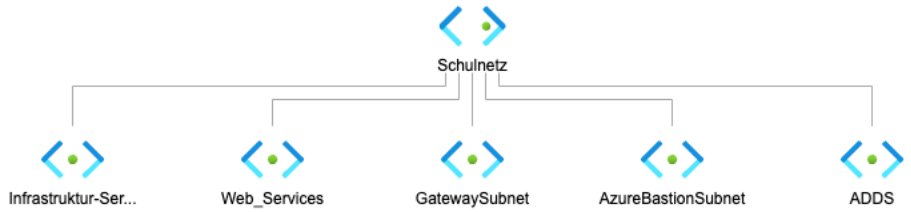
Laborübung 19 - AUFBAU DER NETZWERKINFRASTRUKTUR

Szenario

Für das Erstellen der Onlinestruktur benötigt man ein oder mehrere virtuelle Netzwerke mit Subnetzen zur logische Gliederung.

kurz & knapp

- VNet
- Subnetze
- NSGs
- ARM Templates



Aufgaben:

1. Erstellen Sie ein virtuelles Netzwerk (VNet) 10.42.0.0/16 unter dem Namen Schulnetz-PROD.
2. Erstellen Sie anschließend folgende Subnetze innerhalb des angelegten VNets:

Subnetz	IP Adressbereich
Infrastruktur-Services	10.42.20.0/24
Web-Services	10.42.30.0/24
GatewaySubnet*	10.42.0.0/24
AzureBastionSubnet*	10.42.0.1/26
ADDS	10.42.10.0/24

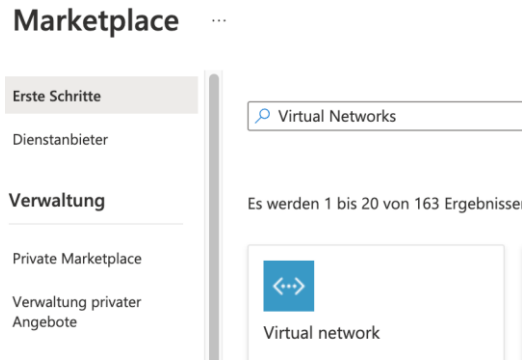
*Name darf nicht geändert werden!

3. Erstellen Sie eine Netzwerksicherheitsgruppe für das Subnetz Web-Services, so dass nur aus der Cloudstruktur auf das Subnetz zugegriffen werden kann.
4. Erstellen Sie gemäß dem RBAC Konzept eine Gruppe „Schulnetz-PROD-Netzwerkadmins“ an und weisen Sie den Mitgliedern dieser Gruppe das Recht „Network Contributor“ zu.

Hinweise

ARM Templates

Das VNET wird über ein ARM Template (Azure Ressource Manager) im Azure Marketplace angelegt. Dies ist der gängige Weg zur Erstellung von Ressourcen. Jede erstellte Ressource muss zwingend einer Subscription/Ressourcegroup/Regin zugeordnet werden, die auch während des Erstellen der Ressource neu angelegt werden kann.



VNet

Ein VNet ist immer einer Region zugeordnet. Sollen mehrere Regionen miteinander kommunizieren benötigt man mehrere VNets (verbuden durch VNet Peering oder VPNs).

DHCP

Jedem Subnetz steht ein transparenter DHCP Server zur Verfügung. Alle Subnetze haben per Default Routing Zugriff aufeinander. Das Internet ist ebenfalls aus allen Subnetzen erreichbar. Microsoft stellt so die grundlegende Kommunikation sicher.

DNS

Standardmäßig steht den Subnetzen ein voll verwalteter, vorkonfigurierter DNS Dienst zur Verfügung.

DDOS Schutz

DDOS Basic ist über die Azure Security Plattform automatisch für alle Ressourcen aktiviert. Überwachung und Abwehr von Angriffen laufen im Hintergrund. Der Dienst wird für alle öffentlichen IP v4/v6 Adressen bereitgestellt

NSGs

Subnetze dienen neben der logischen Gliederung einer Struktur auch als Netzwerksicherheitsgrenzen, die über zugeordnete Network Security Groups konfiguriert werden können. Hier werden ein – und ausgehende Regeln für jede Art von Datenverkehr aus

den Subnetzen und dem Internet erstellt. Eine NSG wird einem oder mehreren Subnetzen zugeordnet.

Gateway Subnetz

Für hybride Infrastrukturen benötigt man ein VPN Gateway, das nur in einem speziellen Subnetz provisioniert werden kann.

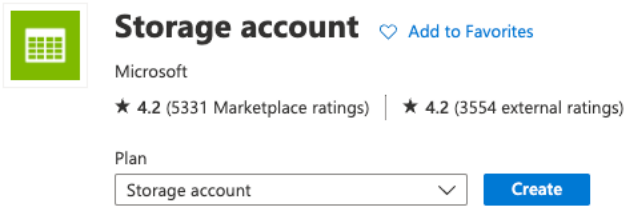
Laborübung 20 - STORAGE ACCOUNT ERSTELLEN

Szenario

Daten sollen online in Microsoft Azure gespeichert werden. Dazu ist ein Storage Account notwendig.

kurz & knapp

- Storage Account
- Storage Typen
- Sync Möglichkeiten



Aufgaben:

1. Erstellen Sie einen Storage Account und weisen Sie diesen Account der Ressource Gruppe Schulnetz-PROD zu:

Ressourcegroupe	Schulnetz-PROD
Storage Account Name	lehrer
Performance	Standard
Redundancy	Locally-redunant storage (LRS)
Zugriff	Aus allen Netzwerken
Routing	Microsoft
Verschlüsselung	Microsoft managed

2. Erstellen Sie eine neue Freigabe „lehrer“ und versuchen Sie darauf zuzugreifen.

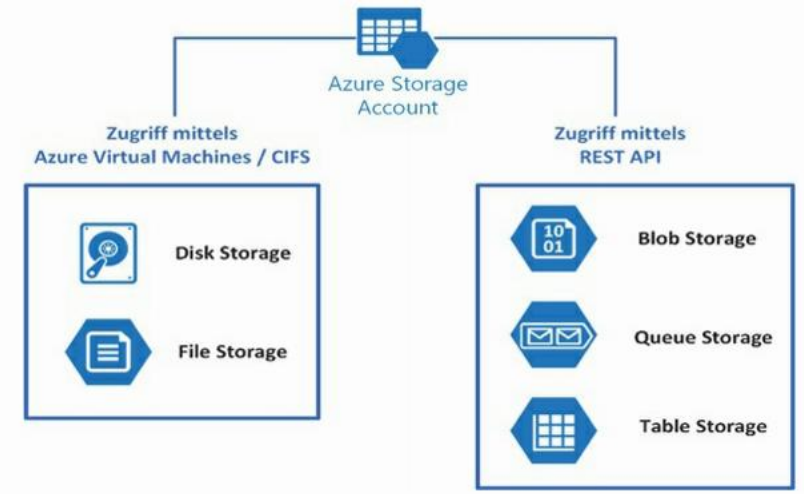
Hinweise

Storage Account

Die Anfangseinstellungen eines Storage Accounts können nicht nachträglich verändert werden. Der Zugriff auf den Account kann über das RBAC-Konzept eingestellt werden.

Generell ist bei der Einrichtung des Storage Accounts Hochverfügbarkeit, Redundanz und Backupstrategie zu berücksichtigen. Alle diese Faktoren erzeugen unterschiedliche Kosten im laufenden Betrieb.

Man unterscheidet zwischen Storage für virtuelle Maschinen (IaaS), für strukturierte Daten wie SQL und für unstrukturierte Daten (BLOBs).



Zugriff auf Storage

BLOB Storage Service: http://‹Name_StorageAccount>.blob.core.windows.net

TABLE Storage Service: http://<Name_StorageAccount>.table.core.windows.net

QUEUE Storage Service: http://<Name_StorageAccount>.queue.core.windows.net

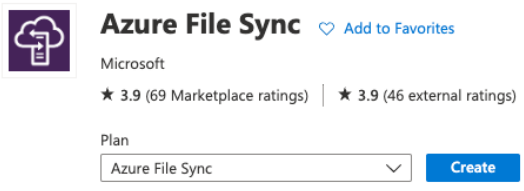
FILE Storage Service : http://<Name_StorageAccount>.file.core.windows.net

Über DNS CName Einträge kann auch ein Zugriff über eigene Domänennamen erfolgen.

Der Zugriff auf eine Ressource ist z.B. mit Access Key und einer REST- API /für Anwendungen) möglich oder über die Ressource ID und einer SMB3 Freigabe. Die jeweiligen Links incl. Verbindungsskripte für Win/macOS/Linux kann man in den Eigenschaften der Freigabe ermitteln.

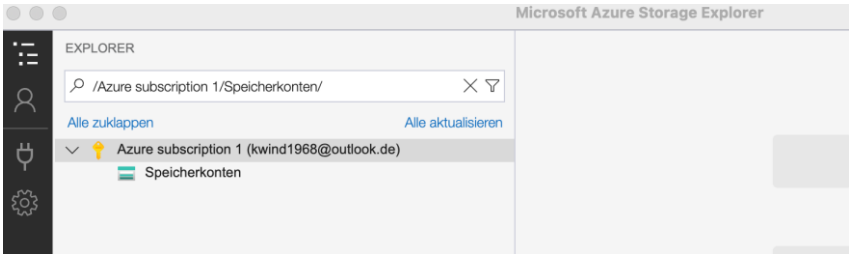
Freigaben

Für alle gängigen Betriebssysteme können Skripte für die Verbindung mit den Freigaben heruntergeladen werden. Bei einer hybriden Struktur können auch lokale Freigaben im AD mit Online Freigaben abgeglichen werden:



Für weitere Syncronisationsvorgänge mit anderen (Cloudspeichern) gibt es ARM Templates im Azure Marketplace.

Azure Storage Manager



https://azure.microsoft.com/en-us/products/storage/storage-explorer/

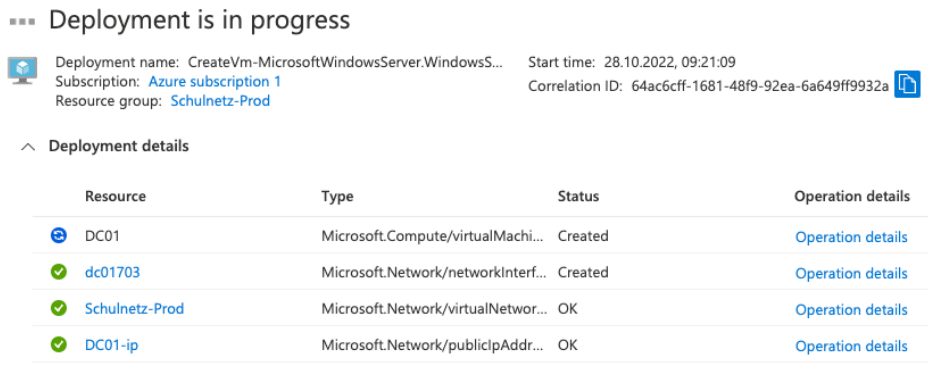
Laborübung 21 - ERSTELLEN EINER VM

kurz & knapp

- VM
- Konfiguration
- ARM Templates

Szenario

In einigen Subnetzen sollen virtuelle Maschinen provisioniert werden. Auf die VMs soll per RDP zugegriffen werden. Dieser Zugriff soll möglichst abgesichert sein.



Aufgaben:

1. Erstellen Sie eine Windows Server VM im Subnetz ADDS!
2. Erstellen Sie eine Windows 11 VM im Subnetz Web-Services!
3. Konfigurieren Sie für beide VMS einen sicheren Zugriff über RDP und führen Sie jeweils die Erstkonfigurationsschritte der Betriebssysteme aus!

Hinweise

Virtuelle Maschinen (VMs)

Virtuelle Maschinen können beim Anlegen manuell konfiguriert werden (Hardware, Netzwerk, öffentliche IP, Verfügbarkeit, Backup Plan, usw.) oder aus vorgefertigten ARM Templates aus dem Azure Marketplace erstellt werden. Es gibt auch Skript Vorlagen, welche komplette Umgebungen (z.B. für Labs zum Testen) in einem Rutsch provisionieren.

Zugriff auf VMs

Jede VM ist aus allen Subnetzen des virtuellen Netzwerks sofort erreichbar (und auch über ein eventuell per VPN angebundenes lokales Netzwerk). Zusätzlich kann man der VM eine öffentliche IP-Adresse zuweisen. Wird über eine NSG der RDP bzw. SSH-Port freigeschaltet, ist die VM direkt aus dem Internet erreichbar. Dies wird jedoch nicht empfohlen.

IP Adressen

Jede VM kann mehrere virtuelle Netzwerkschnittstellen besitzen. Damit sind auch eigene Sicherheitsszenarien (z.B. der Einsatz von UTMs oder Security Appliances) realisierbar.

Regionen

Die VM kann nur auf Ressourcen zugreifen, die sich in derselben Ressourcengruppe und Region befinden!

Azure Bastion Host

Azure Bastion Host ist ein vollständig verwalteter PaaS Dienst, der den sicheren Zugriff auf VMs innerhalb eines VNet aus dem Internet realisiert und ist die bessere Lösung für den RDP-Zugriff. Für jedes VNet ist eine eigene Instanz des Bastion Host Service notwendig. Zusätzlich muss in jedem VNet ein eigenes Subnetz für den Bastion Host konfiguriert werden.

ANHANG

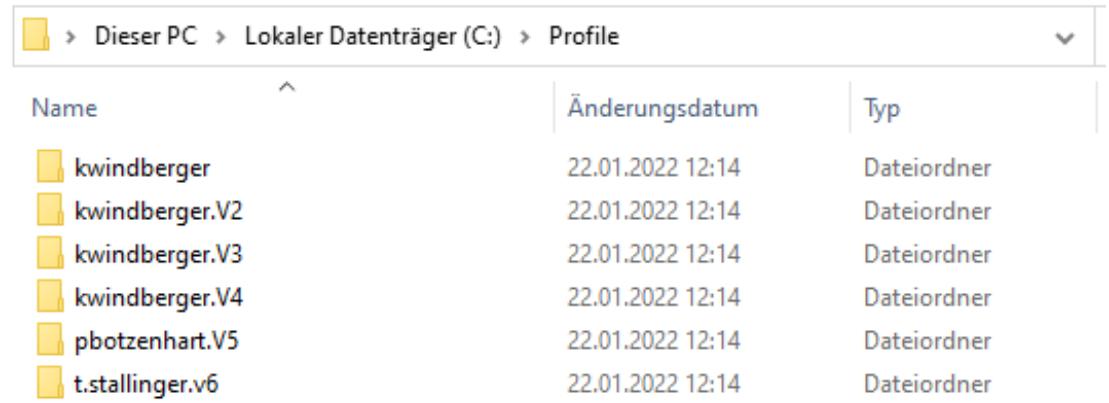
Servergespeicherte Profile

Servergespeicherte Profile oder auch „**Roaming Profiles**“ kamen im Windows Server Umfeld immer dann zum Einsatz, wenn Anwender und Benutzer in Schulen wechselnde PC-Arbeitsplätze hatten, also der klassische Fall von Schulklassen in Computerräumen.

Alle Benutzerprofileinstellungen wurden im servergespeicherten Profil auf dem Anmeldeserver gespeichert (Desktop, Startmenu, Hintergrund, Ordnerumleitungen) und bei einer Anmeldung an einem Client auf diesen geladen.

Jede Veränderung an dem Profil wird dann beim Abmelden im servergespeicherten Profil auf den Anmeldeserver zurückgesichert. Probleme bereiten hier oft spezielle Applikationen, die im Benutzerprofil Einstellungsdateien speichern oder auch die Größe des Profils (Es kann mehrere GB groß werden, was An- und Abmeldung stark verzögert).

Leider benutzt Microsoft mit jeder Version des Clients Betriebssystems, von dem sich ein Benutzer anmeldet eine andere Profilstruktur, die untereinander nicht kompatibel sind und mit Versionsnummern gekennzeichnet werden.



In dem Ordner \Profile auf dem Server, auf dem die servergespeicherten Profile abgelegt werden, gibt es dann mehrere Benutzerprofilordner. Das bedeutet, dass für jede Windows Version als Client Betriebssystem ein neues Benutzerprofil angelegt werden muss, wobei die neuere Client Betriebssystemversion sich die Einstellungen aus der älteren Version holt und in das neue Format konvertiert. Hier treten oft große Schwierigkeiten auf!

Bisher wurde seit Windows Vista für jedes größere Windows-Update eine neue Profilstruktur eingeführt.

Profilversionen bisher (die Endung wird an den Benutzerprofilordner angehängt):

Profilversion	**Betriebssystem**
	Windows XP
.V2	Vista, Windows 7, Server 2008 (R2)
.V3	Windows 8 und Server 2012
.V4	Windows 8.1 und Server 2012 R2
.V5	Windows 10 RTM, Windows 10 1511
.V6	Windows 10 1607, 1703, 1709, 1803, 1809, 1903,1909 bis ?

Servergespeicherte Profile können generell also nur noch reibungslos funktionieren, wenn man sicherstellen kann, dass sich Benutzer nur von Clients an der Domäne anmelden, die denselben Versionsstand besitzen. Verwendet eine Schule BYOD Szenarien oder mobile Dienstgeräte ist dies unrealistisch.

Die Verwendung von servergespeicherten Profilen wird von Microsoft nicht mehr aktiv weiterentwickelt („deprecated“). Es haben sich Nachfolgetechnologien etabliert, die die Verwendung dieser Profile ersetzen sollen.

Die **User Experience Virtualization** (UE-V) kann benutzerdefinierte Windows- und Anwendungseinstellungen aufzeichnen und auf einem zentral verwalteten Netzlaufwerk speichern. Wenn sich Benutzer anmelden, werden ihre persönlichen Einstellungen für ihre Sitzung übernommen, unabhängig davon, an welchem Gerät die Anmeldung erfolgt. UE-V basiert auf der Verwendung von **Microsoft Configuration Designer** und der Erstellung von **Bereitstellungspaketen**. Leider gibt es auch bei UE-V schon zwei Versionen und es ist nicht klar, ob Microsoft diese Technologie in zukünftigen Versionen weiter entwickeln wird. Der Trend geht hier zu zentralen Verwaltungslösungen (evtl. cloudbasiert) wie Intune oder Endpoint Manager im Rahmen eines Microsoft Azure Abonnements.

Verbindliche Profile

Verbindliche Profile oder „**Mandatory Profiles**“ sind schreibgeschützte Profile, die Benutzern zugewiesen werden können. Meldet sich ein Benutzer am Server an, so wird eine Kopie dieses Profils verwendet. Allerdings werden alle Änderungen beim Abmelden nicht zurückgespeichert und der Benutzer erhält immer wieder eine originale Kopie des ursprünglichen Profils.

Mehrere Benutzer können dieses Profil problemlos gleichzeitig benutzen. Umzusetzen ist diese verbindliche Profil sehr einfach. Das Profil wird auf einem Verzeichnis auf dem Server gespeichert und den jeweiligen Benutzern zugewiesen (Eigenschaften). Zusätzlich muss die Datei user.dat in user.man umbenannt werden.

Standard-Netzwerkbenutzerprofil

Sollen alle Anwender (oder eine bestimmte Benutzergruppe) in der Domäne das gleiche Profil bei der ersten Anmeldung erhalten, kann dieses Profil auf einem Domänencontroller abgelegt werden:

1. Melden Sie sich an einem Windows 11 PC mit dem Benutzerkonto an der Domäne an, das als Standardprofil dienen soll.
2. Nehmen Sie alle Einstellungen vor, die Sie für das Profil festlegen wollen (Hintergrund, Freigaben, etc.)
3. Melden Sie sich ab und melden Sie sich an demselben PC mit einem Domänenadministratorkonto an.
4. Erstellen Sie in der NETLOGON Freigabe auf dem Domänencontroller ein Verzeichnis „Default User.v2“.
5. Öffnen Sie die Systemeigenschaften (sysdm.cpl), „Erweitert“ und markieren Sie den Benutzer, dessen Profil Sie als Standard verwenden wollen.
6. Wählen Sie „Kopieren nach“ und kopieren Sie das gesamte Profil in den eben erstellten Ordner in NETLOGON.
7. Im Bereich Benutzer „Andere“ auswählen, geben Sie „Jeder“ ein und überprüfen Sie den Namen.
8. Bestätigen Sie alle noch offenen Fenster. Das Profil wird in die Freigabe kopiert.

In einigen Fällen ist die Schaltfläche „Kopieren nach“ nicht verfügbar. Dann kann das Profil per Hand über den Explorer kopiert werden. Dabei muss man aber versteckte und Systemdateien (eventuell ausgeblendet) mit berücksichtigen. Die Benutzergruppe (im

Beispiel „Jeder“), welche das Profil verwenden soll, benötigt das *Ändern* Recht im Profilordner!

Das Profil wird bei der ersten Anmeldung des Benutzers aus der NETLOGON Freigabe kopiert und dann im Profilpfad des Benutzers gespeichert. Der Benutzer kann das Profil verändern.

Windows Netzwerkumgebung

Windows versucht in der Netzwerkumgebung alle PCs und Geräte eines Windows-Netzwerkes anzuzeigen und benutzt dabei eine Reihe von Protokollen, die standardmäßig an jeden Netzwerkadapter zusammen mit dem TCP/IP v4 Protokoll gebunden sind. Dazu gehört die *Verbindungsschicht Topologie Erkennung* und auch *UPnP*.

Doch der Hauptbestandteil der aufgelisteten Geräte stammt - vor allem in älteren Versionen von Windows - vom „Computerbrowserdienst“, der Bestandteile der SMB Version 1 benutzt, die in Netzwerken aus Sicherheitsgründen nicht mehr verwendet werden sollte.

Microsoft bietet hier eine eigene Lösung an, damit PCs im Windows Netzwerk gefunden werden.

Einige Dienste sollten auf einem Windows PC unbedingt laufen, damit von ihm freigegebene Ressourcen wie Drucker oder Freigaben im Netzwerk gefunden werden können. Dazu gehören

- Arbeitsstationsdienst
- Server
- Datei – und Druckerfreigabe
- Client für Microsoft Netzwerke

Gerade in heterogenen Windows Netzwerken ist die Anzeige der Netzwerkressourcen in der Netzwerkumgebung leider alles andere als zuverlässig.

Windows Server – DNS in AD integriert

In einem klassischen Windows Server Netzwerk wird die Namensauflösung nicht mehr über NetBIOS Namen über einen WINS Server durchgeführt, sondern über DNS. Sollte hier der Zugriff auf Freigaben über die Netzwerkumgebung nicht funktionieren, so kann das andere Gründe haben (z.B. Firewall Einstellungen).

Windows Arbeitsgruppen

Auch ohne lokalen DNS-Server müssen Windows PCs eine Namensauflösung durchführen. Während hier der Zugriff auf das Internet durch den DNS-Proxy des Providers normalerweise keine Probleme bereitet, sieht es im lokalen Netzwerk oft anders aus. Wurde DNS nicht konfiguriert (Primäres Domänensuffix), so greift ein Windows PC auf eine Namensauflösung über NetBIOS zurück. Die Anzeige in der Netzwerkumgebung gleicht hier eher einem Glücksspiel.

Heterogene (Windows) Netzwerke

Ein „Durcheinander“ in der Namensauflösung kann z.B. passieren, wenn

- mehrere PCs in verschiedenen Arbeitsgruppen auf gemeinsame Freigaben zugreifen oder eine Windows Domäne denselben Namen wie eine Arbeitsgruppe besitzt (z.B. alp10.local und alp10)
- bei Virtualisierungen ein virtuelles (Server -) Netzwerk mit dem Host und echten PCs über virtuelle Schnittstellen kommuniziert,
- ältere Geräte keine Auflösung über DNS beherrschen oder nicht konfiguriert wurden (NAS Boxen, Drucker, Samba Server).

In diesen Situationen kann die Installation eines WINS Servers zusätzlich zum DNS-Server helfen, obwohl Microsoft WINS Server als „*Legacy-Registrierungs- und Auflösungsdienst für Computernamen, der NetBIOS-Computernamen IP-Adressen zu ordnet*“ bezeichnet.

WINS Server

Ein WINS Server im lokalen Netzwerk benötigt kaum Ressourcen und ist eigentlich unnötig, wenn alle Clients im Netzwerk ausschließlich eine saubere DNS-Namensauflösung durchführen würden. Dies ist in den wenigsten Netzwerken der Fall.

Wird stattdessen eine Namensauflösung über NetBIOS durchgeführt und es gibt keinen WINS Server im Netzwerk, so werden diese Namensauflösungen durch Broadcasts durchgeführt.

Ein WINS Server verringert also Broadcasts im lokalen Netzwerk. Dabei gibt es eine Hierarchie bei der Namensauflösung:

- Anfrage an den primären WINS Server

- Anfrage an einen (eventuell vorhandenen) zweiten WINS Server
- Broadcast
- LMHOSTS Datei

Netzwerkumgebung ausblenden

In domänenbasierten Netzwerken kann die Netzwerkumgebung mit einer Gruppenrichtlinie ausgeblendet werden. Auf Freigaben und Drucker wird dann durch Zuordnung über Anmeldeskripte oder Gruppenrichtlinien zugegriffen. In diesem Falle kann NetBIOS auch deaktiviert werden. Allerdings muss sichergestellt werden, dass der Zugriff auf Nicht-Domänenmitglieder weiterhin möglich ist.

Auch ohne Namensauflösung sollte ein Zugriff über den UNC-Pfad mit IP-Adresse z.B. \\10.36.104.26\schulnetz möglich sein. Dies ist aber für Endanwender sehr umständlich.

NetBIOS Knotentypen

Eine NetBIOS Namensauflösung weist einem PC-Namen eine IP-Adresse zu und umgekehrt. Auf welche Weise dies geschieht, legt der Knotentyp fest:

Knotentyp	Erklärung	Auflösungsversuch über
B - Knoten	B = Broadcast	Broadcast
P - Knoten	P = Peer to Peer	WINS Server, kein Broadcast
M - Knoten	M = Mixed	Broadcast, dann WINS Server
H - Knoten	H = Hybrid	WINS Server, dann Broadcast

Der Knotentyp wird automatisch ermittelt oder besser per DHCP eingestellt. Ein Windows Server ist z.B. ein B – Knoten und wird zu einem H – Knoten, wenn auf ihm das WINS Server Feature installiert wird. Wie oben beschrieben kann auch die LMHOSTS Datei ausgewertet werden.